The Arithmetic-Geometric Mean and Periods of Curves of Genus 1 and 2

By

Rudolf Wing Tat Chow

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

School of Mathematics and Statistics
The University of Sheffield

April 2018

Abstract

When Gauss discovered the arithmetic-geometric mean (AGM) around 1800, it was a seemingly harmless iterative process which could compute some kind of elliptic integrals. Little could he expect that a century later his work would become one of the fastest algorithm to compute the digits of π. In more modern number theory, it has been used to compute periods of elliptic curves over $\mathbb{C}$, extended to p-adic fields and even generalised to curves of genus 2.

This thesis expands on the generalisation of the AGM to genus 2 curves over $\mathbb{C}$ and p-adic fields. After giving an introduction and some background knowledge on the work of Gauss, it is split into three parts:

1. We present an algorithm to compute the periods of a hyperelliptic curve over $\mathbb{C}$. This closely resembles the method described by Bost and Mestre in [BM88], but adapted with some subtle differences.

2. After a survey of the work by [HM89], in which they modify Gauss' AGM to p-adic fields and devise an algorithm to compute the preimage of a point in its Tate curve, we then show how this can be used to compute some type of p-adic Coleman integrals.

3. We devise an AGM process for curves of genus 2 over p-adic fields, drawing ideas from both of the above. The ultimate aim is to have a quadratically convergent algorithm to compute the preimage of a point in its Mumford uniformisation. In particular, this can be used to compute periods associated to the hyperelliptic curve. Details of the final step of the algorithm are missing from this thesis, but will (hopefully!) be published in a joint paper with Frazer Jarvis in due time.

Acknowledgements

"If I have seen further it is by standing on the shoulders of Giants."

– Issac Newton

First and foremost, I would like to thank my supervisor Frazer Jarvis. Without his patience and continuous encouragements in the past years this work would not have been possible; his expertise on this area has provided me with insights time and time again. It has been a privilege to work under Frazer. In particular I appreciate the time and effort he spent in translating several key papers from French to English despite his duties as senior tutor.

I also wish to thank every one of my colleagues and friends, from Sheffield to London, Hong Kong and beyond. The number theory group here in Sheffield has provided a welcoming environment for me to learn and broaden my perspective. I have my advisor Haluk Sengun to thank especially, who has organised several learning seminars throughout the years on top of giving me advices.

It goes without saying that I am beyond grateful for my family's support (including our two absolutely adorable cats – without whom this thesis might have been completed a little earlier!). They have allowed me to follow my desires and stood by me regardless of the choices I made throughout my life.

Contents

Introduction

The arithmetic-geometric mean (AGM) is a quadratically convergent iterative process that is extremely simple to implement: given two positive real numbers, at each stage one simply evaluates their arithmetic and geometric means, which is where the name originated from. It was in fact first published by Lagrange (see [Cox84]), but it was Gauss who first analysed and realised its importance in computing elliptic integrals efficiently – for which it is still used today. Even so, it was largely forgotten for the most part of the next century.

It was not until the late twentieth century that it gained popularity, when the advances in technology were met with a growing interest in computational mathematics. Brent suggested in his paper [Bre76] that it can be used to compute elementary transcendental functions such as e^x and $\sin x$; the two Borwein brothers even published an entire book titled '*Pi and the AGM*'. From there, Bost and Mestre generalised it to genus 2 in [BM88] before Henniart and Mestre adapted it to p-adic fields in [HM89] – the list of applications probably far exceeded what Gauss foresaw. It is perhaps the simplicity of the algorithm combined with the elegant yet profound algebraic geometry interpretations behind it that makes for such an intriguing area to study.

Chapter 1 serves as an introduction to the background of the subject, starting with Gauss' discovery of the link between the genus 1 AGM and elliptic integrals. Theta functions, which play a key role throughout this thesis, are also introduced. The main reference up to this point is Cox's paper [Cox84]. We also present a modern account of the theory from the paper [CT13] by Cremona and his student Thongjunthug. It re-interprets the work of Gauss using the theory of lattice chains and modular forms. The chapter ends on a slight digression on the classical Landen transformation to motivate the work in parts of Chapters 3 and 4.

Chapter 2 begins with a survey of the theory of hyperelliptic curves and associated objects such as their Jacobians and period matrices. We also cover some classical tools such as Thomae's formula. Moving onto the generalised AGM, we discuss two such versions found in the literature. A four variable version by Jarvis in [Jar08] has applications such as the computation of determinants of period matrices; whereas a six variable alternative by Bost and Mestre can compute period matrices. The situation over $\mathbb{R}$ is well understood in [BM88], and we extend their algorithm to $\mathbb{C}$. Although the algorithm was not explicitly written down in their paper, one cannot help but feel that this was probably known to Bost and Mestre already. With that in mind, perhaps the most important result here is Theorem 2.27, which gives a different perspective to the algorithm: period doubling. The algorithm has also been implemented using Magma.

Chapter 3 returns to elliptic curves, but shifting to p-adic fields. The primary aim of this chapter is to explain the Tate uniformisation of elliptic curves and the p-adic AGM found in [HM89]. The AGM is used to compute preimages inside the Tate curve with an algorithm which Henniart and Mestre call the non-archimedean analogue of the descending Landen transformation. Their paper also gives a method to compute the period of an elliptic curve. We end on a surprising application of this AGM in computing certain types of Coleman integrations. This chapter should serve as motivation for Chapter 4.

Chapter 4 delves into the theory of p-adic hyperelliptic curves, combining the efforts of the last two chapters. It begins with an overview of the uniformisation theory involving Mumford curves and Schottky groups following [GvdP80] and [Kad07]. With these preliminaries covered, we can describe how the Bost-Mestre AGM adapts into the p-adic world for certain totally split curves. One of the main results is that, as in Chapter 2, the AGM process in fact doubles the periods (or rather, squares the multiplicative periods). In the last part of the work, we describe a strategy that can be used to mimic the p-adic Landen transformation; it is largely built on the theory laid in Teitelbaum's paper [Tei88]. Details of the first half of this algorithm are given and we close with an example of how it works in practice with the modular curve $X_0(23)$.

The appendices contain all the codes from Sage, Magma and Pari that were used throughout this thesis.

Chapter 1

The Arithmetic-Geometric Mean

1.1 Gauss and the AGM

Given two positive real numbers a and b with $a \geq b$, we define two corresponding sequences (a_n) and (b_n) by first setting $a_0 = a$ and $b_0 = b$, then using the iterative algorithms

$$a_{n+1} = \frac{a_n + b_n}{2} \quad \text{and} \quad b_{n+1} = \sqrt{a_n b_n} \ .$$

That is to say, a_{n+1} and b_{n+1} are the arithmetic and geometric mean of the pair (a_n, b_n) respectively. For example, by setting $a = \sqrt{2}$ and $b = 1$, the first few iterations of the sequences are shown below:

$$\begin{array}{rclrcl}
a_0 &=& 1.41421356237309504880168872 & b_0 &=& 1 \\
a_1 &=& 1.20710678118654752440084436 & b_1 &=& 1.18920711500272106671749997 \\
a_2 &=& 1.19815694809463429555917210 & b_2 &=& 1.19812352149312012260658550 \\
a_3 &=& 1.19814023479387720908287880 & b_3 &=& 1.19814023467730720579838370 \\
a_4 &=& 1.19814023473559220744063130 & b_4 &=& 1.19814023473559220743921360 \\
a_5 &=& 1.19814023473559220743992240 & b_5 &=& 1.19814023473559220743992240
\end{array}$$

It is easy to see that these two sequences converge to the same limit; whence we define the *arithmetic-geometric mean* (AGM) of a and b to be this common limit, denoted $M(a, b)$. In fact, since

$$a_{n+1} - b_{n+1} = \frac{\left(\sqrt{a_n} - \sqrt{b_n}\right)^2}{2} = \frac{(a_n - b_n)^2}{2\left(\sqrt{a_n} + \sqrt{b_n}\right)^2} \leq \frac{1}{8b_1}(a_n - b_n)^2 \ ,$$

we see that this convergence is in fact quadratic (that is, the number of correct digits roughly

doubles every iteration). This concept was first recorded by Gauss; he discovered that this AGM is closely related to elliptic integral of the first kind, namely that

Theorem 1.1. *If $a \geq b > 0$, then*

$$I(a,b) := \int_0^{\frac{\pi}{2}} \frac{d\phi}{\sqrt{a^2\cos^2\phi + b^2\sin^2\phi}} = \frac{\pi}{2M(a,b)} \ .$$

An elementary proof uses the ingenious change of variable

$$\sin\phi = \frac{2a\ \phi'}{(a+b)+(a-b)\sin^2\phi'} \ ,$$

which then the AGM preserves the integral such that

$$I(a,b) = I(a_1,b_1) = I(a_2,b_2) = \cdots \ .$$

Details can be found in Theorem 1.1 of [Cox84].

The situation is more interesting when one starts out with an initial pair of complex numbers. Of course at any stage there are two possible square roots for b_{n+1}, which means that for any pair of initial values one would obtain uncountably many corresponding sequences, making the AGM a multi-valued function. Fortunately, Proposition 2.1 in [Cox84] shows that all possible sequences converge regardless of the choices made at any step and only countably many of these limits are non-zero.

While at first glance there seems not to be a natural or correct choice of square root in the geometric mean, Gauss was able to completely determine all possible values of any given initial pair of complex numbers. If $a, b \in \mathbb{C}^\times$ are complex numbers such that $a \neq \pm b$, then say that a square root B of ab is the *right choice* if $|A-B| \leq |A+B|$, where A is the arithmetic mean of a and b. If $|A-B| = |A+B|$, we also require that $\mathrm{Im}(B/A) > 0$.

If a and b are both positive and real, it seems natural to always pick the positive square root. And indeed, one quickly checks that the above definition does agree with our intuition. The definition of a right choice also gives rise to a *simplest value* of the AGM, $M(a,b)$, which is the value taken by the AGM if the right choice of square root is made at every stage. The importance of this lies in the following theorem, which determines all possible values the AGM can take given an initial pair:

Theorem 1.2. *Let $a, b \in \mathbb{C}^\times$ satisfying $a \neq \pm b$ and $|a| \geq |b|$. Then μ is a value of the AGM of a and b if and only if there exist coprime integers $c \equiv 0 \mod 4$ and $d \equiv 1 \mod 4$ such that*

$$\frac{1}{\mu} = \frac{d}{M(a,b)} + \frac{ic}{M(a+b, a-b)} \ .$$

These were all proved by Gauss, who essentially employed the theory of modular forms without explicitly writing it down. For details of the proof see Theorem 2.2 in [Cox84].

1.2 Theta Functions

Let z and τ be complex numbers such that τ lies in the upper half plane $\mathbb{H}$. Define the *theta function* (in genus 1 – which refers to z and τ being numbers rather than vectors and matrices) to be the summation

$$\theta(z, \tau) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau + 2\pi i n z} \ .$$

This is sometimes called the *Jacobi* or *Riemann theta function* for historical reasons. Recall that any elliptic curve (up to rescaling) can be considered as a lattice Λ generated by 1 and τ, where τ lies in the upper half plane. For this reason we often refer to this as the theta function of genus 1. The summation is entire in z and holomorphic in τ; furthermore it converges absolutely and uniformly on compact sets, since for any fixed τ and z we have

$$\sum_{n \in \mathbb{Z}} \left| e^{\pi i n^2 \tau + 2\pi i n z} \right| \leq \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \operatorname{Im} \tau + 2\pi n |z|} < \sum_{n \geq N} e^{-\frac{1}{2} \pi n^2 \operatorname{Im} \tau}$$

for some N such that $e^{-\pi N^2 \operatorname{Im} \tau + 4\pi N |z|} < 1$. The function was defined such that it would have certain periodicity properties with respect to the complex lattice generated by 1 and τ. Explicitly, replacing z by $z + 1$ we immediately see that the function is $\mathbb{Z}$-periodic, that is,

$$\theta(z, \tau) = \theta(z + 1, \tau) \ .$$

Secondly if we let z go to $z + \tau$, we see that

$$\theta(z + \tau, \tau) = e^{-\pi i \tau - 2\pi i z} \theta(z, \tau) \ ,$$

which together gives the transformation law

$$\theta(z + s\tau + t, \tau) = e^{-\pi i s^2 \tau - 2\pi i s z} \theta(z, \tau)$$

for any integers s and t. Now let $a, b \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Define the theta functions *with characteristics* to be the functions

$$\theta_{2a,2b}(z,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i(n+a)^2\tau + 2\pi i(z+b)(n+a)} \ .$$

It is straightforward to check that these are also quasi-periodic with respect to 1 and τ, that is

$$\begin{aligned}\theta_{2a,2b}(z+m,\tau) &= e^{2\pi i a m}\theta_{2a,2b}(z,\tau),\\ \theta_{2a,2b}(z+m\tau,\tau) &= e^{-2\pi i b m - \pi i m^2\tau - 2\pi i m z}\theta_{2a,2b}(z,\tau) \ .\end{aligned}$$

In genus 1 there are four possible characteristics, but all of them are essentially translations of the original theta functions along with some non-vanishing factor:

$$\begin{aligned}\theta_{0,0}(z,\tau) &= \theta\left(z,\tau\right) \ ,\\ \theta_{0,1}(z,\tau) &= \theta\left(z+\frac{1}{2},\tau\right) \ ,\\ \theta_{1,0}(z,\tau) &= e^{\frac{1}{4}\pi i\tau + \pi i z}\theta\left(z+\frac{\tau}{2},\tau\right) \ ,\\ \theta_{1,1}(z,\tau) &= e^{\frac{1}{4}\pi i\tau + \pi i\left(z+\frac{1}{2}\right)}\theta\left(z+\frac{\tau}{2}+\frac{1}{2},\tau\right) \ .\end{aligned}$$

With a moment's thought one immediately notices that $\theta_{0,0}$, $\theta_{0,1}$ and $\theta_{1,0}$ are even in z whereas the function $\theta_{1,1}$, on the other hand, is odd in z. For example, we have

$$\begin{aligned}\theta_{1,1}(-z,\tau) &= \sum_{n\in\mathbb{Z}} e^{\pi i\left(n+\frac{1}{2}\right)^2\tau + 2\pi i\left(n+\frac{1}{2}\right)\left(-z+\frac{1}{2}\right)}\\ &= \sum_{n\in\mathbb{Z}} e^{\pi i\left(-n-\frac{1}{2}\right)^2\tau + 2\pi i\left(-n-\frac{1}{2}\right)\left(-z+\frac{1}{2}\right)}\\ &= \sum_{n\in\mathbb{Z}} e^{\pi i\left(n+\frac{1}{2}\right)^2\tau + 2\pi i\left(n+\frac{1}{2}\right)\left(z+\frac{1}{2}\right) - 2\pi i\left(n+\frac{1}{2}\right)}\\ &= -\theta_{1,1}(z,\tau)\end{aligned}$$

and the others are similar. By slight abuse of language we say that the characteristic $[a,b] \in (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^2$ is odd (even respectively) if its corresponding theta function is odd (even respectively). Equivalently this means that $[a,b]$ is odd if and only if $4ab$ is an even integer. Since the different theta functions are all translations of each other, this allows us to easily study the zeros of these functions.

Proposition 1.3. *The zeros of $\theta_{a,b}(z,\tau)$ are the points*

$$z = \Lambda + \left(a + \frac{1}{2}\right)\tau + \left(b + \frac{1}{2}\right) \ .$$

Furthermore the four different theta functions do not have common zeros.

Proof. This is Lemma 4.1 in Chapter I of [Mum83]. Firstly by an exercise in counting zeros by contour integration we see that each $\theta_{a,b}$ has exactly four zeros inside 2Λ, where Λ is the lattice $\mathbb{Z} + \tau\mathbb{Z}$. The idea is that it is sufficient to study $\theta_{1,1}$, which we know has a zero at $z = 0$. By the translation

$$\theta_{1,1}(z,\tau) = e^{\frac{1}{4}\pi i\tau + \pi i\left(z+\frac{1}{2}\right)}\theta_{0,0}\left(z + \frac{\tau}{2} + \frac{1}{2}, \tau\right) \ ,$$

we know that $\theta_{0,0}$ vanishes at $(\frac{\tau}{2} + \frac{1}{2})$ and so we can account for all four zeros inside 2Λ. Finally translating these points we get the zeros of the other theta functions as desired. □

In fact this holds true for the vector space generated by the four theta functions in that the elements in any basis have no common zeros. One important geometric application of these theta functions is that they can be used to embed complex tori. For a lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau \in \mathbb{H}$, we define the map $\phi : \mathbb{C}/\Lambda_\tau \to \mathbb{P}^3$ that maps

$$\phi(z) = [\theta_{0,0}(z,\tau) : \theta_{0,1}(z,\tau) : \theta_{1,0}(z,\tau) : \theta_{1,1}(z,\tau)] \ .$$

Theorem 1.4. *The map ϕ is a holomorphic embedding (that is, injective and non-vanishing derivative at every point).*

Proof. We provide a quick sketch of the proof here following of [Mum83]. The first thing to note is that this is well defined. By the previous proposition, we know that the theta functions do not vanish simultaneously, and by replacing z by $z + \lambda$ for some $\lambda \in \Lambda$, this simply multiplies every theta function by some non-zero factor (namely $e^{-\pi i\tau - 2\pi iz}$) and hence gives the same point inside the projective space. Since each of the theta functions is holomorphic, the map ϕ itself is also holomorphic.

Suppose that there exists some z_1 and z_2 such that $\phi(z_1) = \phi(z_2)$ (the case where derivative vanishes at a point is identical). By the quasi-periodicity we can always translate these points by some $a\tau + b$ with a and b half integers to get a distinct pair of points z_1' and z_2'

inside 2Λ such that $\phi(z_1') = \phi(z_2')$. But this allows us to construct a linear combination

$$f = \lambda_1\theta_{0,0} + \lambda_2\theta_{0,1} + \lambda_3\theta_{1,0} + \lambda_4\theta_{1,1}$$

such that f vanishes at z_1, z_1' and z_3 for another distinct point z_3, since we have three linear equations in four unknowns. But now $\phi(z_1) = \phi(z_2)$ means that f also vanishes at z_2 and z_2', giving a total of five zeros in 2Λ, which is a contradiction. □

1.3 AGM and Elliptic Functions

The point of interest to us here is the link between AGM and periods of elliptic curves. Let us, for now, consider an elliptic curve of the form $y^2 = P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, where we assume $e_1 < e_2 < e_3$ are real numbers. Then by periods we simply mean integrals of the form

$$\omega_1 = 2\int_{e_1}^{e_2} \frac{dx}{\sqrt{P(x)}} \quad \text{and} \quad \omega_2 = 2i\int_{e_2}^{e_3} \frac{dx}{\sqrt{P(x)}} \ .$$

These are in fact nothing more than path integrals on closed loops of a complex torus; we will discuss the basics of these in more generality when we study curves of higher genus in the next chapter. By evaluating the theta functions from the last section at $z = 0$ one obtains the three functions (since the fourth function is odd and vanishes at $z = 0$)

$$\begin{aligned}
\theta_{0,0}(\tau) &= \theta(0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2} \ , \\
\theta_{0,1}(\tau) &= \theta\left(\frac{1}{2},\tau\right) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2} \ , \\
\theta_{1,0}(\tau) &= \theta\left(\frac{\tau}{2},\tau\right) = \sum_{n\in\mathbb{Z}} q^{\left(n+\frac{1}{2}\right)^2} \ ,
\end{aligned}$$

where $q = e^{\pi i\tau}$. Of course $\theta_{0,0}^k$, for k odd, are famous examples of half-integral weight modular forms (of level 4 and trivial character) which are interesting in their own right, but our focus is much simpler. An elementary calculation shows that the squares of these theta functions behave like the AGM when τ is doubled, in the sense that one has

$$\theta_{0,0}(2\tau)^2 = \frac{\theta_{0,0}(\tau)^2 + \theta_{0,1}(\tau)^2}{2} \quad \text{and} \quad \theta_{0,1}(2\tau)^2 = \sqrt{\theta_{0,0}(\tau)^2\theta_{0,1}(\tau)^2} \ .$$

These are examples of duplication formulae for theta functions, which have been well understood over the years. For now we will simply quote these results; but a more detailed

discussion of these will follow in the next chapter. Therefore setting $a_0 = \theta_{0,0}(\tau)^2$ and $b_0 = \theta_{0,1}(\tau)^2$ yields the AGM sequence where $a_n = \theta_{0,0}(2^n\tau)^2$ and $b_n = \theta_{0,1}(2^n\tau)^2$. This, combined with the observation that $\theta_{0,0}$ and $\theta_{0,1}$ both tend to 1 as $\operatorname{Im}\tau$ tends to infinity, implies that

$$M(\theta_{0,0}(\tau)^2, \theta_{0,1}(\tau)^2) = 1 \ .$$

Next recall the Weierstrass $\wp$-function associated with a complex lattice $\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\gamma \in \Gamma \setminus \{0\}} \left[\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right] \ ,$$

which acts as a bijection between the elliptic curve with periods ω_1 and ω_2, and the torus $\mathbb{C}/\Gamma$. Similarly, by setting $\tau = \omega_1\omega_2^{-1}$ such that $\operatorname{Im}\tau > 0$, one gets the corresponding lattice $\widetilde{\Gamma} = \mathbb{Z} + \mathbb{Z}\tau$ and Weierstrass function $\widetilde{\wp}$ (so that $\widetilde{\wp}(z) = \omega_1^2\wp(\omega_1 z)$). It was shown in [Mum83] (combining pages 26 and 64) that one may construct *all* $\widetilde{\Gamma}$-meromorphic functions (that is, meromorphic functions $f(z)$ such that $f(z+\tau) = f(z)$ for all $\tau \in \widetilde{\Gamma}$) using exponential and quotients of theta functions. In particular, we have

$$\widetilde{\wp}(z) = c - \pi^2 e^{-2\pi i z}\theta(1/2,\tau)^2\theta(\tau/2,\tau)^2 \frac{\theta(z,\tau)^2}{\theta(z+(\tau+1)/2,\tau)^2}$$

for some constant c. Letting $z = 1/2$, $\tau/2$ and $(\tau+1)/2$, we get the identities

$$\begin{aligned} \pi^2\theta_{0,0}(\tau)^4 &= \widetilde{\wp}(1/2) - \widetilde{\wp}(\tau/2) \ , \\ \pi^2\theta_{0,1}(\tau)^4 &= \widetilde{\wp}(1/2) - \widetilde{\wp}((\tau+1)/2) \end{aligned}$$

when taking into account $\theta_{0,1}(\tau)^4 + \theta_{1,0}(\tau)^4 = \theta_{0,0}(\tau)^4$ (also known as Jacobi's identity, which we will prove in the next chapter) and $\theta((\tau+1)/2,\tau) = 0$. Piecing everything together gives

$$\begin{aligned} \omega_1^2 e_3 &= \omega_1^2\wp(\omega_1/2) = \widetilde{\wp}(1/2) \ , \\ \omega_1^2 e_2 &= \omega_1^2\wp((\omega_1+\omega_2)/2) = \widetilde{\wp}((\tau+1)/2) \ , \\ \omega_1^2 e_1 &= \omega_1^2\wp(\omega_2/2) = \widetilde{\wp}(\tau/2) \ , \end{aligned}$$

and thus

$$\omega_1\sqrt{e_3 - e_1} = \pi\theta_{0,0}(\tau)^2 \quad \text{and} \quad \omega_1\sqrt{e_2 - e_1} = \pi\theta_{0,1}(\tau)^2 \ .$$

By taking the AGM of the two equations we have proven the first part of

Theorem 1.5. *If $e_1 < e_2 < e_3$ are the three distinct real roots of an elliptic curve, then its periods ω_i are given by*

$$\omega_1 = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \quad \textit{and} \quad \omega_2 = \frac{i\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})} \ .$$

The second part is done analogously.

1.4 Elliptic Curves over $\mathbb{C}$ and Towers of Isogeny

With a little effort, similar formulae can be found for elliptic curves with complex coefficients. This can, for example, be found in [CT13], whose method resembles that of Gauss. The idea is to reinterpret the change of variation in the proof of Gauss' theorem as a morphism between two related elliptic curves, and thus the AGM is essentially constructing a tower of elliptic curves.

Starting with an elliptic curve E_0 defined by $y^2 = 4(x - e_1^{(0)})(x - e_2^{(0)})(x - e_3^{(0)})$, where the Weierstrass points are now complex numbers such that $e_1^{(0)} + e_2^{(0)} + e_3^{(0)} = 0$, first we set $a_0 = \sqrt{e_1 - e_3}$ with arbitrary sign and $b_0 = \pm\sqrt{e_1 - e_2}$, where the sign of b_0 is chosen such that $|a_0 - b_0| \leq |a_0 + b_0|$. Using the AGM sequence $\{(a_n, b_n)\}$ we define a corresponding sequence of elliptic curves $\{E_n\}$ with roots

$$e_1^{(n)} = \frac{a_n^2 + b_n^2}{3}, \quad e_2^{(n)} = \frac{a_n^2 - 2b_n^2}{3} \quad \text{and} \quad e_3^{(n)} = \frac{b_n^2 - 2a_n^2}{3} \ .$$

For $n \geq 1$, one finds a 2-isogeny (a surjective morphism with finite kernel) φ_n between E_n and E_{n-1} defined by

$$\begin{aligned} x_{n-1} &= x_n + \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{x_n - e_3^{(n)}} \ , \\ y_{n-1} &= y_n \left(1 - \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{(x_n - e_3^{(n)})^2}\right) \ . \end{aligned}$$

Let $\dfrac{dx_n}{y_n}$ be the canonical differential associated to the elliptic curve E_n. Then by directly taking derivatives of the equations above one see that

$$\varphi^* \left(\frac{dx_{n-1}}{y_{n-1}}\right) = \frac{dx_n}{y_n} \ .$$

Since $E_n(\mathbb{C}) \cong \mathbb{C}/\Lambda_n$, where Λ_n is the period lattice of the differential $\dfrac{dx_n}{y_n}$, we get a commutative diagram as follows:

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & \mathbb{C} & \longrightarrow & \mathbb{C} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & \mathbb{C}/\Lambda_n & \longrightarrow & \mathbb{C}/\Lambda_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \wp_n} & & \downarrow{\scriptstyle \wp_{n-1}} & & \\
\cdots & \longrightarrow & E_n & \xrightarrow{\varphi_n} & E_{n-1} & \longrightarrow & \cdots
\end{array}$$

Next, define a *chain of lattices of index 2* to be a sequence of lattices (Λ_n) which satisfies the conditions

1. $\Lambda_n \supseteq \Lambda_{n+1}$ for all $n \geq 0$;
2. $[\Lambda_n : \Lambda_{n+1}] = 2$ for all $n \geq 0$;
3. $\Lambda_{n+1} \neq 2\Lambda_{n-1}$ for all $n \geq 1$.

So intuitively these are just sequences of lattices in the complex plane that eventually extend infinitely in one direction. For any $n \geq 1$, the sublattice $\Lambda_{n+1} \subseteq \Lambda_n$ is the *right choice* if $\Lambda_{n+1} = \langle w \rangle + 2\Lambda_n$ for some minimal element $w \in \Lambda_n \setminus 2\Lambda_{n-1}$ (with respect to the complex norm). We say a lattice chain (and similarly an AGM sequence) is good if the right choice is made at all but finitely many steps; the chain is optimal if every step is right. The key lies in the following proposition, taken from Theorem 10 of [CT13]:

Proposition 1.6. *For all $n \geq 0$, we have*

1. *Λ_{n+2} is the right choice of sublattice of Λ_{n+1} (i.e. $\Lambda_{n+1} = \langle \omega \rangle + 2\Lambda_n$) if and only if (a_n, b_n) is the right choice.*
2. *The lattice chain (Λ_n) is good (respectively, optimal) if and only if the sequence $\{(a_n, b_n)\}$ is good (respectively, optimal).*

The proof gives a link between the lattice chains, chains of elliptic curves and their corresponding modular form structures. Finally, one can show by direct computation that

$$\lim_{n\to\infty} \wp_{\Lambda_n}(z) = \left(\frac{\pi}{\omega_1}\right)^2 \left(\frac{1}{\sin^2(z\pi/\omega_1)} - \frac{1}{3}\right) .$$

Since $\wp_{\Lambda_n}\left(\dfrac{\omega_1}{2}\right) = e_1^{(n)}$, one gets, as in Theorem 1.5,

Theorem 1.7. *Let E is an elliptic curve defined by $y^2 = 4(x - e_1^{(0)})(x - e_2^{(0)})(x - e_3^{(0)})$ such that $e_1^{(0)} + e_2^{(0)} + e_3^{(0)} = 0$ and set $a_0 = \sqrt{e_1 - e_3}$ and $b_0 = \pm\sqrt{e_1 - e_2}$ as above. Then we have*

$$\omega_1 = \frac{\pi}{M(a_0, b_0)} \ .$$

Combining these ideas one obtains an algorithm to compute periods of elliptic curves:

Algorithm 1.8 (Computing a period lattice basis)**.**
Input: An elliptic curve E over $\mathbb{C}$ with roots $e_i \in \mathbb{C}$ for $i = 1, 2, 3$ such that $e_1 + e_2 + e_3 = 0$.
Ouput: Three periods of E, any two of which form a $\mathbb{Z}$-basis for the period lattice of E.

1. *Label one of the roots as e_1 and the other two arbitrarily as e_2 and e_3.*
2. *Set $a_0 = \sqrt{e_1 - e_3}$ with arbitrary sign and $b_0 = \pm\sqrt{e_1 - e_2}$, where the sign of b_0 is chosen such that $|a_0 - b_0| \leq |a_0 + b_0|$.*
3. *Compute $\omega = \dfrac{\pi}{M(a_0, b_0)}$ using the simplest value of the AGM.*
4. *Repeat by setting each of the other two roots as e_1.*

These are taken from Corollary 16 and Algorithm 20 in [CT13] respectively.

1.5 Descending Landen Transformation

We end on a slight digression on an application of the AGM (which we will consider a slightly different p-adic version of it later). The Landen transformation is a mapping of the parameters of an elliptic integral, widely used for computing elliptic functions numerically. It was originally due to Landen (which did not involve the AGM) and independently rediscovered later by Gauss. It can also be interpreted as inverting the Abel-Jacobi map and lifting points from the elliptic curve to its Jacobian, which we will introduce with more details in the next chapter. We include the proof of it here for completeness' sake. Let

$$I = \int_u^\infty \frac{dx}{\sqrt{(x - e_1)(x - e_2)(x - e_3)}} \ ,$$

where the e_i are real numbers such that $e_1 < e_2 < e_3$, $e_1 + e_2 + e_3 = 0$ and $u > e_3$. Then we have the following:

Algorithm 1.9 (Landen Transformation)**.**
Input: An elliptic curve E with roots $e_i \in \mathbb{R}$ for $i = 1, 2, 3$ such that $e_1 < e_2 < e_3$ and a real number $u > e_3$.
Ouput: Value of the integral

$$I = \int_u^\infty \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}} \ .$$

1. *Let* $a_0 = \sqrt{e_3 - e_1}$, $b_0 = \sqrt{e_3 - e_2}$ *and* $x_0 = u$.

2. *Apply the AGM to* (a_0, b_0). *That is, for* $n \geq 1$, *let*

$$\begin{aligned} a_n &= \frac{a_{n-1} + b_{n-1}}{2} \ , \\ b_n &= \sqrt{a_{n-1} b_{n-1}} \ , \\ x_n &= \frac{1}{2}\left(x_{n-1} - \frac{a_{n-1}^2 + b_{n-1}^2}{6} + \sqrt{\left(x_n + \frac{a_{n-1}^2 + b_{n-1}^2}{6} \right)^2 - \left(\frac{a_{n-1}^2 - b_{n-1}^2}{2} \right)^2} \right) \ . \end{aligned}$$

3. *Denote the limits of the sequences* $\{a_n\}$ *and* $\{x_n\}$ *by* $M(a_0, b_0)$ *and* X *respectively. Then the original integral* I *is given by*

$$I = \frac{2}{M(a_0, b_0)} \left(\frac{\pi}{2} - \tan^{-1}\left(\frac{\sqrt{X - \frac{2}{3} M(a_0, b_0)^2}}{M(a_0, b_0)} \right) \right) \ .$$

Furthermore, by considering the change of variable

$$x = \frac{e_2 x' - e_2 e_3 + e_1 e_3 - e_1 e_2}{x' - e_2} \ ,$$

one can apply the algorithm to integrals of the form

$$I' = \int_u^{e_2} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}}$$

with $e_1 \leq u \leq e_2$.

Proof. Let $a_0 = \sqrt{e_3 - e_1}$ and $b_0 = \sqrt{e_3 - e_2}$. Denote by a_1 and b_1 the arithmetic and geometric mean of a_0 and b_0 respectively. Setting

$$e_1' = \frac{b_1^2 - 2a_1^2}{3} \ , \quad e_2' = \frac{a_1^2 - 2b_1^2}{3} \quad \text{and} \quad e_3' = \frac{a_1^2 + b_1^2}{3} \ ,$$

we see that $e_1' < e_2' < e_3'$ and $e_1' + e_2' + e_3' = 0$. Now consider the change of variable (this is, of course, the same isogeny we saw in the last section)

$$x = x' + \frac{(e_1' - e_3')(e_1' - e_2')}{x' - e_1'} \ ,$$

which gives the identity

$$\int_{x_0}^{\infty} \frac{dx}{\sqrt{(x - e_1)(x - e_2)(x - e_3)}} = \int_{u}^{\infty} \frac{dx}{\sqrt{(x - e_1')(x - e_2')(x - e_3')}} \ ,$$

where we have

$$x_0 = u + \frac{(e_1' - e_3')(e_1' - e_2')}{u - e_1'} = u + \frac{-3a_1^2(b_1^2 - a_1^2)}{3u - (b_1^2 - 2a_1^2)} \ .$$

Solving the quadratic for u one sees that

$$\begin{aligned}
u &= \frac{1}{2}\left(x_0 + \frac{b_1^2 - 2a_1^2}{3} + \sqrt{\left(x_0 + \frac{b_1^2 - 2a_1^2}{3}\right)^2 + 4\left(a_1^2(b_1^2 - a_1^2) - x_0\frac{b_1^2 - 2a_1^2}{3}\right)}\right) \\
&= \frac{1}{2}\left(x_0 + \frac{b_1^2 - 2a_1^2}{3} + \sqrt{\left(x_0 - \frac{b_1^2 - 2a_1^2}{3}\right)^2 + 4(a_1^2)(b_1^2 - a_1^2)}\right) \\
&= \frac{1}{2}\left(x_0 - \frac{a_0^2 + b_0^2}{6} + \sqrt{\left(x_0 + \frac{a_0^2 + b_0^2}{6}\right)^2 - \left(\frac{a_0^2 - b_0^2}{2}\right)^2}\right) \\
&= x_1
\end{aligned}$$

since

$$\frac{b_1^2 - 2a_1^2}{3} = \frac{a_0 b_0 - \frac{1}{2}(a_0 + b_0)^2}{3} = -\frac{a_0^2 + b_0^2}{6}$$

and

$$4a_1^2(b_1^2 - a_1^2) = \left(a_0 b_0 - \left(\frac{a_0 + b_0}{2}\right)^2\right)\left(\frac{a_0 + b_0}{2}\right)^2 = -\left(\frac{a_0^2 - b_0^2}{2}\right)^2 \ .$$

By iterating the above process, one obtains a sequence of elliptic curves. As n tends to

infinity, the curves tend to the cubic

$$y^2 = 4\left(x - \frac{2}{3}M(a_0,b_0)^2\right)\left(x + \frac{1}{3}M(a_0,b_0)^2\right)^2 ,$$

which can be parameterised by

$$x = t^2 + \frac{2}{3}M(a_0,b_0)^2 \quad \text{and} \quad y = 2t(t^2 + M(a_0,b_0)^2) .$$

Finally, letting $t = M(a_0,b_0)\tan\phi$, we have $d\phi = M(a_0,b_0)\dfrac{dx}{y}$ and hence

$$2\int_{x_\infty}^{\infty} \frac{dx}{\left(x + \frac{1}{3}M(a_0,b_0)^2\right)\sqrt{x - \frac{2}{3}M(a_0,b_0)^2}} = 2\int_{y_\infty}^{\frac{\pi}{2}} \frac{d\phi}{M(a_0,b_0)} ,$$

where

$$y_\infty = \tan^{-1}\left(\frac{t}{M(a_0,b_0)}\right) = \tan^{-1}\left(\frac{\sqrt{(X - \frac{2}{3}M(a_0,b_0)^2)}}{M(a_0,b_0)}\right)$$

and we are done. □

Chapter 2

Generalisation to Genus 2

We now turn to the study of a genus 2 generalisation of the AGM, following the work of [BM88] amongst several others. But before we can delve into the details, we first provide some introduction to the theory of hyperelliptic curves in general (even though we are only concerned about genus 2 here) and some relevant tools in the study.

2.1 Hyperelliptic Curves and Their Jacobians

A hyperelliptic curve is an algebraic curve given by an equation of the form

$$C : y^2 = (x - a_1)(x - a_2) \cdots (x - a_d) = x^d + b_{d-1}x^{d-1} + \cdots + b_1 x + b_0 \ ,$$

where $a_i \in \mathbb{C}$ (or any field of odd characteristic) are all distinct. If the curve has genus g geometrically, then the degree is given by $d = 2g + 1$ or $2g + 2$. Any hyperelliptic curve is endowed with the involution that maps the point (x, y) to $(x, -y)$. By making the branch cuts (a_{2i}, a_{2i+1}) on two copies of $\mathbb{P}^1(\mathbb{C})$ (i.e. taking a double covering of $\mathbb{P}^1(\mathbb{C})$ ramified over the a_i's) and gluing them together, one can also view this as a Riemann surface. If the degree of the equation is odd then there is a branch point at infinity.

Similar to an elliptic curve, one can define a group law on the points of a hyperelliptic curve akin to the chord and tangent method. This is done by simply replacing points by groups of g points and replacing lines by interpolating polynomials (so that rigorously speaking this is a group law on the Jacobian of the curve – an object we will define very shortly). For simplicity we assume that $g = 2$. Given two pairs of points $[P_1, P_2]$ and $[Q_1, Q_2]$, there exists generically a unique cubic (counted with multiplicity if any of the four points coin-

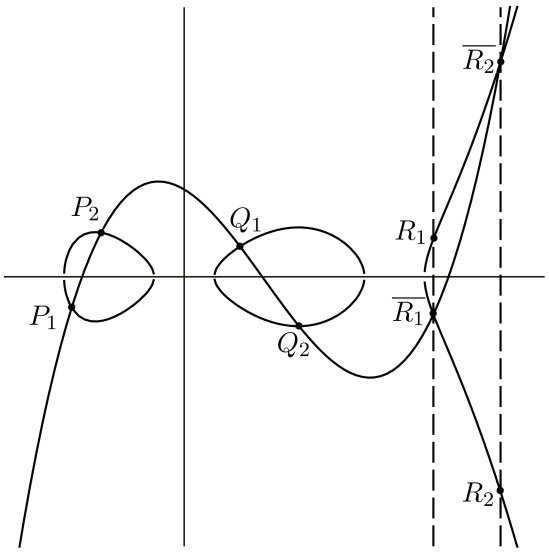

Figure 2.1: Group law for a genus 2 hyperelliptic curve

cides) that passes through the four points. Now intersecting this cubic with the curve gives two extra roots, say $\overline{R_1}$ and $\overline{R_2}$. Then define the sum $P_1 + P_2 + Q_1 + Q_2$ as the involution of these two points (see Figure 2.1 above). Explicit formulae can be found in [Lei05].

The *first homology group* $H_1(C, \mathbb{Z})$, measuring the 1-dimensional holes on the surface, is essentially the set of closed paths on the surface; a set of $2g$ non-homologous cycles $\{a_i, b_i\}$, $i = 1, ..., g$ is a *symplectic basis* if their intersection indices satisfy

$$a_i \circ a_j = 0, \quad b_i \circ b_j = 0 \quad \text{and} \quad a_i \circ b_j = \delta_{ij}$$

for all i, j, where δ_{ij} is the Kronecker delta. The following is an example of a symplectic basis for a hyperelliptic curve of genus 3:

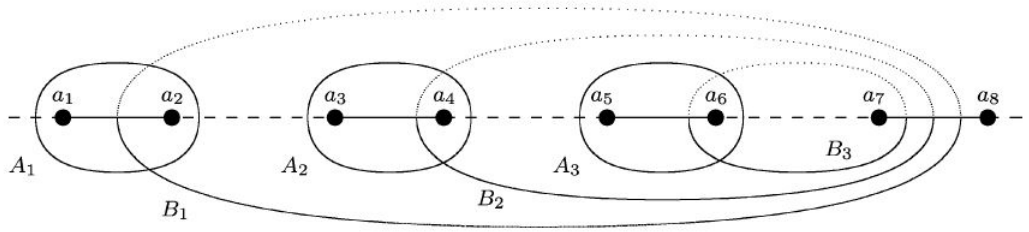

Figure 2.2: A symplectic basis for a genus 3 hyperelliptic curve

Note that symplectic bases are by no means unique. The complementary object associated to this homology group is the vector space of holomorphic 1-forms. For a hyperelliptic curve in the above form, this is simply spanned by $du_i = x^i \frac{dx}{y}$ for $i = 0, ..., g-1$ (see Chapter 3.7 in [FK80]). The *periods* (of the first kind) are obtained by integrating these 1-forms along closed loops. It is known from the Riemann bilinear relations that these periods form a lattice $\Lambda \subseteq \mathbb{C}^g$. The Jacobian $J(C)$ of the curve is defined by the quotient $J(C) = \mathbb{C}^g/\Lambda$. It is a principally polarised abelian variety and thus a complex torus of real dimension $2g$.

A *divisor* is a finite linear combination of points on the curve with integer coefficients, and the degree of such a divisor is the sum of its coefficients. Those divisors that are divisors of meromorphic functions are called *principal*. The set of all degree 0 divisors, denoted $\mathrm{Div}^0(C)$, clearly forms an abelian group under addition, and the set of all principal divisors, denoted $\mathrm{Div}^P(C)$, forms a subgroup. We now describe the Jacobian variety $J(C)$ in terms of these divisor groups.

Fix a base point p_0 on the curve C. For a generic point $p \in C$, define the *Abel-Jacobi map* $\mu : C \to J(C)$ which sends p to the point

$$\mu(p) = \left(\int_{p_0}^{p} du_1, \int_{p_0}^{p} du_2, \ldots, \int_{p_0}^{p} du_g \right) \mod \Lambda$$

and we extend this definition to divisors on C simply by linearity. The fundamental result of Abel and Jacobi is that this map defines an isomorphism between divisors and the Jacobian (historically injectivity was proved by Abel and surjectivity by Jacobi). A proof of the theorem can be found in Chapter 3.6 of [FK80].

Theorem 2.1. *The Abel-Jacobi map is an isomorphism between the Jacobian and the quotient of degree 0 divisors by principal divisors. That is,*

$$J(C) \cong \mathrm{Div}^0(C)/\mathrm{Div}^P(C) \ .$$

Meromorphic differentials (or differentials of the second kind) of a hyperelliptic curve with a degree $2g+1$ model has a basis given in page 195 of [Bak97]

$$dr_j = \sum_{k=j}^{2g+1-j} (k+1-j) b_{k+1+j} \frac{x^k dx}{4y}$$

for j from 1 to g. Integrals of these differentials along closed loops on the curve are called

periods of the second kind. But for our purposes we will mostly focus on periods of the first kind.

Given a hyperelliptic curve and any symplectic basis, we split the periods into two types, purely for convenience: with reference to Figure 2.2 above, Type A-periods are those obtained by integrating a closed loop around two branch points (i.e. the cycles A_i), and Type B-periods are those which circle the entire Riemann surface (i.e. the cycles B_i). Furthermore, denote ω_{ij} and ω'_{ij} to be the periods obtained by integrating du_i along the paths A_j and B_j respectively. In this case one obtains two $g \times g$ matrices $\Omega_1 = (\omega_{ij})_{i,j=1}^{g}$ and $\Omega_2 = (\omega'_{ij})_{i,j=1}^{g}$. Adjoining these together we obtain the $g \times 2g$ (big) *period matrix* $\begin{pmatrix}\Omega_1 & \Omega_2\end{pmatrix}$. Similarly we denote η and η' to be the matrices obtained by integrating the periods of the second kind along A_j and B_j respectively.

Note that the columns of the big period matrix are exactly the basis of the lattice Λ which defines the Jacobian. This is of particular interest of study due to Torelli's theorem, which states that the period matrix completely determines the Riemann surface, up to isomorphism, in the case of a principally polarised abelian variety (Theorem 12.1 in [CS86]). It is always possible to choose a specific basis of the cohomology such that $\Omega_1 = I_g$, and in this case one can prove that the corresponding Ω_2 is a Riemann matrix (that is, symmetric with positive definite imaginary part, whence it lies in the Siegel upper half plane). We call Ω_2 the *small period matrix*. Given any big period matrix $\begin{pmatrix}\Omega_1 & \Omega_2\end{pmatrix}$, one can obtain a small period matrix by computing $\Omega_1^{-1}\Omega_2$. It is important to note that neither the big nor the small period matrices are unique, since the path that is integrated along can be extended by any linear combinations of the loops. But any two small period matrices are equivalent under the action of some $2g \times 2g$ symplectic matrix (more on the symplectic group will be explained in the next section).

Finally, it is well known from the Riemann bilinear relations (see [Mum83]) that the matrices Ω_1, Ω_2, H_1 and H_2 satisfy the generalised Legendre relation

$$\begin{pmatrix}\Omega_1 & \Omega_2 \\ H_1 & H_2\end{pmatrix}^{\mathrm{T}} \begin{pmatrix}0 & I_n \\ -I_n & 0\end{pmatrix} \begin{pmatrix}\Omega_1 & \Omega_2 \\ H_1 & H_2\end{pmatrix} = -\frac{\pi i}{2} \begin{pmatrix}0 & I_n \\ -I_n & 0\end{pmatrix} ,$$

where H_1 and H_2 are the matrices of the periods of the second kind, defined similarly to Ω_i.

2.2 Symplectic Matrices

The study of elliptic curves, when viewed as lattices in $\mathbb{C}$ parameterised by some τ in the upper half planne, leads naturally to the study of $\mathrm{SL}_2(\mathbb{Z})$, the set of 2×2 integral matrices with determinant 1. Similarly when one studies the theory of hyperelliptic curves, the matrices naturally associated become the *symplectic matrices*, as briefly hinted in the last section. Hence we make a quick detour to document the basic properties of these groups.

Let F be a field. The *symplectic group of degree* n, denoted $\mathrm{Sp}_{2n}(F)$, is the group of matrices $\gamma \in \mathrm{GL}_{2n}(F)$ such that

$$\gamma^{\mathrm{T}} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \gamma = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} .$$

Clearly if γ is symplectic then

$$(\gamma^{-1})^{\mathrm{T}} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \gamma^{-1} = - \left[\gamma \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \gamma^{-1} \right]^{\mathrm{T}} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

so these matrices do indeed form a group. $\mathrm{Sp}_{2n}(F)$ is in fact an algebraic group that appears naturally as the group of automorphisms of lattices $\mathbb{Z}^{2n} \subseteq \mathbb{C}^n$. If we write any symplectic matrix γ in four $n \times n$ blocks

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} ,$$

then direct computation shows that γ is symplectic if and only if $A^{\mathrm{T}}C$ and $B^{\mathrm{T}}D$ are symmetric and $A^{\mathrm{T}}D - C^{\mathrm{T}}B = I_n$. Just as an example, when $n = 1$ we immediately see that $\mathrm{Sp}_2(F) = \mathrm{SL}_2(F)$, which follows from the above characterisation. For our purposes F is taken to be either $\mathbb{R}$ or $\mathbb{C}$ here (or $\mathbb{Q}_p$ in the last chapter). In particular we are interested in the matrices with integer coefficients, which will be denoted by $\mathrm{Sp}_{2n}(\mathbb{Z})$. Note that $\mathrm{Sp}_{2n}(\mathbb{Z}) = \mathrm{Sp}_{2n}(\mathbb{R}) \cap \mathrm{Mat}_{2n}(\mathbb{Z})$.

While $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half of the complex plane $\mathbb{H}$, the symplectic matrices act on the *Siegel upper half plane*, denoted $\mathbb{H}_n$. This is the set of all n by n symmetric complex matrices with positive definite imaginary part. The action on the Siegel upper half plane is completely analogous to the action on the standard upper half complex plane. Let $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a symplectic matrix and τ be a point in the Siegel upper half plane. Then

we define the action (sometimes called the *generalised Möbius transformation*) by

$$\gamma\tau = (A\tau + B)(C\tau + D)^{-1} \ .$$

It is not immediately obvious that this is a well-defined action; we give a proof following [Sie64].

Lemma 2.2. *The action of* $\mathrm{Sp}_{2n}(F)$ *on* $\mathbb{H}_n$ *is well-defined.*

Proof. Take $\tau \in \mathbb{H}_n$. Then by definition we have $\tau^{\mathrm{T}} - \tau = 0$ and $\frac{1}{2i}(\tau - \overline{\tau}) > 0$, or equivalently we have

$$\begin{pmatrix} \tau^{\mathrm{T}} & I \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} \tau \\ I \end{pmatrix} = \mathbf{0} \quad \text{and} \quad -\frac{1}{2i} \begin{pmatrix} \overline{\tau} & I \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} \tau \\ I \end{pmatrix} > 0 \ .$$

Now if $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2n}(F)$ then one has $\gamma \begin{pmatrix} \tau \\ I \end{pmatrix} = \begin{pmatrix} A\tau + B \\ C\tau + D \end{pmatrix} = \begin{pmatrix} E \\ F \end{pmatrix}$, implying that

$$\begin{pmatrix} E^{\mathrm{T}} & F^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} E \\ F \end{pmatrix} = \begin{pmatrix} \tau^{\mathrm{T}} & I \end{pmatrix} \gamma^{\mathrm{T}} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \gamma \begin{pmatrix} \tau \\ I \end{pmatrix} = \mathbf{0}$$

and similarly

$$-\frac{1}{2i} \begin{pmatrix} \overline{E} & \overline{F} \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} E \\ F \end{pmatrix} > 0 \ .$$

This is equivalent to saying

$$E^{\mathrm{T}}F = F^{\mathrm{T}}E \quad \text{and} \quad -\frac{1}{2i}\left(\overline{E}F - \overline{F}E\right) > 0 \ .$$

To show that $F = (C\tau + D)$ is invertible, suppose v satisfies $Fv = \mathbf{0}$. This implies that $\overline{v}^{\mathrm{T}}\overline{F} = \mathbf{0}$ and $\frac{1}{2i}\overline{v}^{\mathrm{T}}(\overline{E}F - \overline{F}E)v = \mathbf{0}$, whence $v = \mathbf{0}$. Finally from $E^{\mathrm{T}}F = F^{\mathrm{T}}E$ we see that EF^{-1} is symmetric and from the other inequality we see that

$$\frac{1}{2i}\left(EF^{-1} - \overline{EF^{-1}}\right) > 0 \ .$$

It follows that $\mathrm{Im}(EF^{-1}) > 0$ and so $\gamma\tau \in \mathbb{H}_n$ as required. □

Note that if γ is a symplectic matrix, then both γ and its negative $-\gamma$ give rise to the same action. Now let $\tau = X + iY$ be a point in $\mathbb{H}_n$. Since the matrices

$$\begin{pmatrix} \sqrt{Y} & 0 \\ 0 & \sqrt{Y}^{-1} \end{pmatrix} \text{ and } \begin{pmatrix} I & X \\ 0 & I \end{pmatrix}$$

are both symplectic, we obtain two corresponding actions that send τ to $\sqrt{Y}\tau\sqrt{Y}$ and $\tau + X$ respectively for all τ. In particular, letting $\tau = iI$ we obtain a map, via composition, that sends iI to $X + iY$. Hence we have

Proposition 2.3. *The action of the symplectic group is transitive on* $\mathbb{H}_n$.

We also have an analogue of the fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane:

Theorem 2.4. *A fundamental domain for* $\mathbb{H}_n/Sp_n(\mathbb{Z})$ *is given by the set of* $Z = X + iY$ *such that*

(i) $|x_{ij}| \leq \frac{1}{2}$ *for all* i, j;

(ii) $|\det(CZ + D)| \geq 1$ *for all* $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(\mathbb{Z})$;

(iii) Y *is Minkowski reduced, that is,* $a^T Y a \geq Y_{ii}$ *for all* $a \in \mathbb{Z}^n$ *with* $\gcd(a_i, \ldots, a_n) = 1$ *and* $Y_{i,i+1} \geq 0$ *for* $i = 1, \ldots, n-1$.

The proof that this is indeed a fundamental domain can be found in [Got59], and again one checks that when $n = 1$ this reduces to the usual fundamental domain on $\mathbb{H}$.

2.3 Theta Functions in Higher Genera

We saw briefly in the previous chapter how theta functions can link the AGM and period integrals. Here we give a proper introduction to these functions in higher genera. This is an old and vast area of mathematics and interested readers should turn to [Igu72] and [Mum83] for a much more comprehensive account of the theory.

In order to generalise the definition of theta functions to higher genera, one simply replaces z by a g-tuple $\mathbf{z} = (z_1, \ldots, z_g) \in \mathbb{C}^g$, and τ becomes a matrix Ω in the Siegel upper half

space $\mathbb{H}_g$. The exact definition is given by the summation

$$\theta(\mathbf{z}, \Omega) = \sum_{\mathbf{n} \in \mathbb{Z}^g} e^{\pi i \mathbf{n}^{\mathrm{T}} \Omega \mathbf{n} + 2\pi i \mathbf{n}^{\mathrm{T}} \cdot \mathbf{z}} \ .$$

This defines a holomorphic function on $\mathbb{C}^g \times \mathbb{H}_g \to \mathbb{C}$ and it converges absolutely and uniformly in $\mathbf{z}$. The proof is identical to the genus 1 case, for example see Proposition 1.1 of Chapter II in [Mum83]. Many of the desired properties carry forward as expected. For example, let Λ_Ω be the lattice $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ sitting inside $\mathbb{C}^g$, that is, it is generated over $\mathbb{Z}$ by the unit vectors and the columns of Ω. Then for any $\mathbf{a}$ and $\mathbf{b} \in \mathbb{Z}^g$, we see that

$$\theta(\mathbf{z} + \mathbf{a}, \Omega) = \theta(\mathbf{z}, \Omega) \quad \text{and} \quad \theta(\mathbf{z} + \Omega\mathbf{a} + \mathbf{b}, \Omega) = e^{-\pi i \mathbf{a}^{\mathrm{T}} \Omega \mathbf{a} - 2\pi i \mathbf{a}^{\mathrm{T}} \mathbf{z}} \theta(\mathbf{z}, \Omega) \ .$$

Again we define theta functions with characteristics to be translations of $\theta(\mathbf{z}, \Omega)$. More precisely, if $\mathbf{a}$ and $\mathbf{b}$ are vectors in $(\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g$, then we define the theta functions with characteristics $\mathbf{a}$ and $\mathbf{b}$ to be the summation

$$\theta \begin{bmatrix} 2\mathbf{a} \\ 2\mathbf{b} \end{bmatrix} (\mathbf{z}, \Omega) = \sum_{\mathbf{n} \in \mathbb{Z}^g} e^{\pi i (\mathbf{n}+\mathbf{a})^{\mathrm{T}} \Omega (\mathbf{n}+\mathbf{a}) \tau + 2\pi i (\mathbf{z}+\mathbf{b})^{\mathrm{T}} (\mathbf{n}+\mathbf{a})} \ .$$

As expected we find that these are merely translations of the original definition

$$\theta \begin{bmatrix} 2\mathbf{a} \\ 2\mathbf{b} \end{bmatrix} (\mathbf{z}, \Omega) = e^{\pi i \mathbf{a}^{\mathrm{T}} \Omega \mathbf{a} + 2\pi i \mathbf{a}^{\mathrm{T}} (\mathbf{z}+\mathbf{b})} \theta(\mathbf{z} + \Omega\mathbf{a} + \mathbf{b}, \Omega) \ .$$

As before, these functions are either odd or even in $\mathbf{z}$. Since the even ones are the ones where $4\mathbf{a}^{\mathrm{T}}\mathbf{b}$ is an even integer, we have $\frac{1}{2}(4^g + 2^g)$ even and $\frac{1}{2}(4^g - 2^g)$ odd theta functions respectively. The situation to embed lattices into projective space is more complicated and we content ourselves by quoting the theorem of Lefschetz (see [Mum74] for a proof):

Theorem 2.5. *If a complex torus possesses a non-degenerate Riemann form, then there exists an embedding, via the theta functions, into the projective space as an algebraic subvariety. Furthermore every complex torus that can be embedded in a projective space is isomorphic to $\mathbb{C}^g/\alpha_\Omega(L)$ for some $\Omega \in \mathbb{H}_g$ and L a lattice in $\mathbb{C}^g$, where $\alpha_\Omega : \mathbb{R}^g \times \mathbb{R}^g \to \mathbb{C}^g$ is the map defined by $\alpha_\Omega(x, y) = \Omega x + y$.*

A *Thetanullwert* or *theta constant* is the restriction of $\theta_{\mathbf{a},\mathbf{b}}(\mathbf{z}, \Omega)$ to $\mathbf{z} = \mathbf{0}$. These are of particular interest for various reasons. For example, the theta functions $\theta\left[\begin{smallmatrix} \mathbf{0} \\ \mathbf{b} \end{smallmatrix}\right](\mathbf{0}, \Omega)$ are examples of half-weight Siegel modular forms (for more details see [DS00] or [Mum83]).

Our focus here is slightly different; we are interested in some of the duplication formulae related to these theta constants. For convenience, we agree on the notation that any theta functions without the $\mathbf{z}$-argument refer to theta constants.

Theta functions, and especially theta constants, have been very well studied. In particular, they satisfy many duplication and transformation formulae which are the main interest to us here. As such we will quote two main theorems which are employed later.

Theorem 2.6. *Let $\Omega \in \mathbb{H}_g$ and $\mathbf{a}, \mathbf{b} \in (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g$. Furthermore let $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ be a matrix with block form*

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} .$$

Then we have

$$\theta \begin{bmatrix} 2\mathbf{a}' \\ 2\mathbf{b}' \end{bmatrix} \left(\begin{pmatrix} A & B \\ C & D \end{pmatrix} \Omega \right) = \kappa(\mathbf{a}, \mathbf{b}, \gamma) \det(C\Omega + D)^{\frac{1}{2}} \theta \begin{bmatrix} 2\mathbf{a} \\ 2\mathbf{b} \end{bmatrix} (\Omega) ,$$

where

$$\begin{bmatrix} \mathbf{a}' \\ \mathbf{b}' \end{bmatrix} = \begin{bmatrix} D\mathbf{a} - C\mathbf{b} + \frac{1}{2}\mathrm{diag}(CD^{\mathrm{T}}) \\ -B\mathbf{a} + A\mathbf{b} + \frac{1}{2}\mathrm{diag}(AB^{\mathrm{T}}) \end{bmatrix}$$

and

$$\kappa(\mathbf{a}, \mathbf{b}, \gamma) = \zeta_\gamma \exp\left(-\pi i \mathbf{a}^{\mathrm{T}} B^{\mathrm{T}} D\mathbf{a} + 2\pi i \mathbf{a}^{\mathrm{T}} B^{\mathrm{T}} C\mathbf{b} - \pi i \mathbf{b}^{\mathrm{T}} AC\mathbf{b} \right)$$

is a constant that is independent of Ω. The ζ_γ in the last expression is an eighth root of unity that depends only on γ.

A proof can be found in Chapter II of [Igu72]. Note that this transformation property allows one to think of theta functions as modular forms. For example, it immediately follows that the function $\theta\left[\begin{smallmatrix} \mathbf{a}_1 \\ \mathbf{b}_1 \end{smallmatrix}\right](\Omega) \cdot \theta\left[\begin{smallmatrix} \mathbf{a}_2 \\ \mathbf{b}_2 \end{smallmatrix}\right](\Omega)$ for any $\mathbf{a}_i, \mathbf{b}_i \in (\frac{1}{n}\mathbb{Z}/\mathbb{Z})^g$ is a modular form of weight 1, level $(n^2, 2n^2)$.

The second theorem concerns the duplication of theta functions, taken from Theorem 2 in Chapter IV of [Igu72]:

Theorem 2.7. *For $\Omega \in \mathbb{H}_g$ and $\mathbf{a}_i, \mathbf{b}_i \in (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g$, we have*

$$\theta \begin{bmatrix} 2\mathbf{a}_1 \\ 2\mathbf{b}_1 \end{bmatrix} (2\Omega) \cdot \theta \begin{bmatrix} 2\mathbf{a}_2 \\ 2\mathbf{b}_2 \end{bmatrix} (2\Omega) = \frac{1}{2^g} \sum_{\mathbf{n} \in (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^g} (-1)^{4\mathbf{a}_1 \cdot \mathbf{n}} \theta \begin{bmatrix} 2(\mathbf{a}_1 + \mathbf{a}_2) \\ 2\mathbf{n} + \mathbf{b}_1 + \mathbf{b}_2 \end{bmatrix} (\Omega) \cdot \theta \begin{bmatrix} 2(\mathbf{a}_1 - \mathbf{a}_2) \\ 2\mathbf{n} + \mathbf{b}_1 - \mathbf{b}_2 \end{bmatrix} (\Omega) .$$

Note that although we restrict ourselves to half-integer characteristics, one can extend the definition to characteristics of any real number and thus the above formula makes sense. This gives duplication formulae for matrix doubling of even theta functions, which we saw is related to the AGM in genus 1.

For example letting $g = 1$, $\mathbf{a}_1 = \mathbf{a}_2$ and $\mathbf{b}_1 = \mathbf{b}_2$ gives the following three relations:

$$\begin{aligned}
\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2\Omega)^2 &= \frac{1}{2} \left(\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\Omega)^2 + \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\Omega)^2 \right) , \\
\theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2\Omega)^2 &= \theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\Omega) \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\Omega) , \\
\theta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (2\Omega)^2 &= \frac{1}{2} \left(\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\Omega)^2 - \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\Omega)^2 \right) .
\end{aligned}$$

We can combine these identities and see that

$$\begin{aligned}
\theta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (2\Omega)^4 &= \frac{1}{4} \left(\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\Omega)^4 + \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\Omega)^4 - 2\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\Omega)^2 \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\Omega)^2 \right) \\
&= \theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2\Omega)^4 - \theta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (2\Omega)^4
\end{aligned}$$

which is known as Jacobi's identity we used previously.

2.4 Thomae's Formula

Thomae's formula is one of the classical results that relate theta constants to branch points of hyperelliptic curves. It was first proved in [Tho70], and a more modern account can be found in section 8 of [Mum84].

Let C be a hyperelliptic curve with roots $a_1, \ldots, a_{2g+1}$, where g is the genus of the curve. We associate each branch point with a point in the Jacobian via the Abel-Jacobi map (where infinity is chosen as the base point)

$$\mathfrak{A}_i = \int_\infty^{a_i} d\mathbf{u} = \Omega \mathbf{a} + \mathbf{b}$$

and we define an associated vector

$$[\mathfrak{A}_i] = \begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix} .$$

The components of these vectors are either 0 or $\frac{1}{2}$ modulo 1. In fact these can be explicitly computed, as shown in Chapter 7.1 of [FK80]:

$$[\mathfrak{A}_{2k+2}] = \frac{1}{2}\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \underbrace{1 & 1 & \cdots & 1}_{k} & 1 & 0 & \cdots & 0 \end{bmatrix},$$

$$[\mathfrak{A}_{2k+1}] = \frac{1}{2}\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \underbrace{1 & 1 & \cdots & 1}_{k} & 0 & 0 & \cdots & 0 \end{bmatrix}$$

for any $k = 0, \ldots, g$ except $[\mathfrak{A}_{2g+2}]$, which corresponds to the point at infinity and hence is identically zero. This way we get characteristics of a theta function for each individual branch point. For example, in the case of genus 2 we get the following six characteristics:

$$[\mathfrak{A}_1] = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad [\mathfrak{A}_2] = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad [\mathfrak{A}_3] = \frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$[\mathfrak{A}_4] = \frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad [\mathfrak{A}_5] = \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \quad [\mathfrak{A}_6] = \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Those with even indices (apart from $\mathfrak{A}_{2g+2}$), that is $\mathfrak{A}_{2n}$ for $1 \leq n \leq g$, correspond to odd theta functions, and the others correspond to even theta functions. Under this notation the vector of Riemann constants is simply defined as the sum of all the even branch points

$$[K_\infty] = \sum_{k=1}^{g} [\mathfrak{A}_{2k}] .$$

The upshot is that the $[\mathfrak{A}_i]$'s form a basis for the characteristics of theta functions in the sense that all 4^g characteristics can be formed by adding these $\mathfrak{A}_i$'s together and that there is a one-to-one correspondence between these characteristics and partitions of the set $\{1, 2, \ldots, 2g+1\}$.

In particular, we are interested in those partitions which divide the set into two. Let S and S^c be a partition of $\{1, 2, \ldots, 2g+1\}$. We define the characteristics corresponding to this partition to be the vector

$$\begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix} = \sum_{i \in S} [\mathfrak{A}_i] + [K_\infty] \ .$$

This is easily demonstrated with an example. Suppose $g = 2$ and consider the partition $\{1, 2, \ldots, 5\} = S \cup S^c = \{1, 2, 3\} \cup \{4, 5\}$. In this case the corresponding characteristics is simply

$$[\mathfrak{A}_1] + [\mathfrak{A}_2] + [\mathfrak{A}_3] + [K_\infty] = [\mathfrak{A}_4] + [\mathfrak{A}_5] + [K_\infty] = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and we write $\theta\{S\} = \theta[\begin{smallmatrix} 10 \\ 01 \end{smallmatrix}](\Omega)$. With these notations, we have the following proposition (credited to Frobenius in Chapter III of [Mum84]).

Proposition 2.8 (Frobenius' Theta Formula)**.** *Let $S = \{1, 3, \ldots, 2g+1\}$ be the set with $g+1$ elements. For all quadruplets $\mathbf{z}_1, \ldots, \mathbf{z}_4 \in \mathbb{C}^g$ and $\mathbf{a}_1, \ldots, \mathbf{a}_4 \in (\frac{1}{2}\mathbb{Z}/\mathbb{Z})^{2g}$ such that*

$$\sum_{i=1}^{4} \mathbf{z}_i = \mathbf{0} \quad \textit{and} \quad \sum_{i=1}^{4} \mathbf{a}_i = \mathbf{0} \mod 1 \ ,$$

we have

$$\sum_{j=1}^{2g+2} e_S(j) \prod_{i=1}^{4} \theta[\mathbf{a}_i + \mathfrak{A}_j](\mathbf{z}_i) = 0 \ ,$$

where

$$e_S(j) = \begin{cases} 1 & \text{if } j \in S \\ -1 & \text{if } j \notin S \ . \end{cases}$$

Note that the set S in the proposition is fixed by our choice of basis $[\mathfrak{A}_i]$. A different choice of basis would yield a corresponding set S. The main interest to us is that the formula gives a vast collection of identities between theta functions, which we will require later.

Note that for a given partition S of the branch points, the corresponding theta function is even if and only if $\#(S) = g + 1 - m$ for m even. For every partition S we will denote its corresponding theta constant by $\theta\{S\}$. The following is the main theorem due to Thomae:

Theorem 2.9 (Thomae's Theorem)**.** *Let C be a hyperelliptic curve of genus g with big period matrix $\Omega_1\mathbb{Z}^2 + \Omega_2\mathbb{Z}^2$ and suppose $S \cup S^c$ is a partition of $\{1, \ldots, 2g+1\}$ such that $\#(S) = g+1$. Then we have*

$$\theta\{S\}(\Omega)^4 = \pm\frac{(\det\Omega_1)^2}{(i\pi)^{2g}} \prod_{i<j\in S}(a_i - a_j) \prod_{i<j\in S^c}(a_i - a_j) \ .$$

We briefly demonstrate one of its many applications here. In genus 1, the determinant $\det\Omega_1$ is just the period ω_1 itself. Hence Thomae's theorem gives the formulae

$$\omega_1\sqrt{e_3 - e_1} = \pi\theta_{0,0}(\tau)^2 \quad \text{and} \quad \omega_2\sqrt{e_2 - e_1} = i\pi\theta_{0,1}(\tau)^2$$

as in Chapter 1. We end with a simple corollary of the theorem.

Corollary 2.10. *Let S and T be two disjoint subsets of $B = \{1, 2, \ldots, 2g+1\}$ of total size $g-1$. Then for any two $k \neq l$ from the set $B \setminus (S \cup T)$ we have*

$$\frac{a_l - a_m}{a_k - a_m} = \varepsilon\frac{\theta\{k \cup S\}^2\theta\{k \cup T\}^2}{\theta\{l \cup S\}^2\theta\{l \cup T\}^2} \ ,$$

where m is the remaining number in B and $\varepsilon^4 = 1$.

Proof. By Thomae's Theorem we see that

$$\begin{aligned}
\frac{\theta\{k \cup S\}^4}{\theta\{l \cup T\}^4} &= \pm\frac{\displaystyle\prod_{i<j\in(k\cup S)}(a_i - a_j) \prod_{i<j\in(k\cup S)^c}(a_i - a_j)}{\displaystyle\prod_{i<j\in(l\cup T)}(a_i - a_j) \prod_{i<j\in(l\cup T)^c}(a_i - a_j)} \\
&= \pm\frac{\displaystyle\prod_{i<j\in(k\cup S)}(a_i - a_j) \prod_{i<j\in(m\cup l\cup T)}(a_i - a_j)}{\displaystyle\prod_{i<j\in(l\cup T)}(a_i - a_j) \prod_{i<j\in(m\cup k\cup S)}(a_i - a_j)} \\
&= \pm\frac{(a_l - a_m)\displaystyle\prod_{i<j\in(m\cup T)}(a_i - a_j)}{(a_k - a_m)\displaystyle\prod_{i<j\in(m\cup S)}(a_i - a_j)}
\end{aligned}$$

and similarly

$$\frac{\theta\{k \cup T\}^4}{\theta\{l \cup S\}^4} = \pm\frac{(a_l - a_m)\displaystyle\prod_{i<j\in(m\cup S)}(a_i - a_j)}{(a_k - a_m)\displaystyle\prod_{i<j\in(m\cup T)}(a_i - a_j)}$$

from which the result follows. □

2.5 Two Generalisations of the AGM

We now turn our attention to the generalisation of the AGM. Two such generalisations have been studied: one, by Jarvis in [Jar08], uses four starting variables whereas the other, by Bost and Mestre in [BM88], uses six. For notational convenience, we fix, once and for all, the following labelling of the ten even theta functions in genus 2:

$$\theta_0(\Omega) = \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (\Omega) \ , \quad \theta_1(\Omega) = \theta \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} (\Omega) \ ,$$

$$\theta_2(\Omega) = \theta \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} (\Omega) \ , \quad \theta_3(\Omega) = \theta \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} (\Omega) \ ,$$

$$\theta_4(\Omega) = \theta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} (\Omega) \ , \quad \theta_5(\Omega) = \theta \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} (\Omega) \ ,$$

$$\theta_6(\Omega) = \theta \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\Omega) \ , \quad \theta_7(\Omega) = \theta \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} (\Omega) \ ,$$

$$\theta_8(\Omega) = \theta \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (\Omega) \ , \quad \theta_9(\Omega) = \theta \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} (\Omega) \ .$$

We also note in passing that we will often switch between working with a quintic model and a sextic model of a hyperelliptic curve, whichever is more convenient in the situation. This is mainly due to historical reasons, where some classical results were proved and more easily applied in one model than the other. But since two such models of the same curve can be obtained via a linear change of variable, this should cause no confusion.

2.5.1 The Four Variable AGM

Jarvis suggested a notion of a genus 2 AGM using four numbers, rediscovering the definition by Borchardt. It can be seen as a generalisation to abelian surfaces (as opposed to hyperelliptic curves as in the other generalisation). The method presented in the paper has the advantages that it is closely connected to genus 2 theta functions. This allows one to prove similar results to those of Gauss in [Cox84], for example determining the set of possible AGM values (in most cases). Another advantage of this notion is the ease of generalisation to even higher genera.

Let $a_0 = a, b_0 = b, c_0 = c$ and $d_0 = d$ be real, positive numbers such that $a_0 \geq b_0 \geq c_0 \geq d_0$, and for $n \geq 1$ define

$$\begin{aligned} a_{n+1} &= \frac{1}{4}(a_n + b_n + c_n + d_n) \ , \\ b_{n+1} &= \frac{1}{2}(\sqrt{a_n b_n} + \sqrt{c_n d_n}) \ , \\ c_{n+1} &= \frac{1}{2}(\sqrt{a_n c_n} + \sqrt{b_n d_n}) \ , \\ d_{n+1} &= \frac{1}{2}(\sqrt{a_n d_n} + \sqrt{b_n c_n}) \ . \end{aligned}$$

The four sequences $\{a_n\}$, $\{b_n\}$, $\{c_n\}$ and $\{d_n\}$ converge to a common limit $M_4(A, B, C, D)$. Note that ordering $a_n \geq b_n \geq c_n \geq d_n$ is preserved for all n and so $A \geq B \geq C \geq D$. This convergence is once again quadratic since

$$\begin{aligned} a_{n+1} - d_{n+1} &= \frac{1}{4}\left[(\sqrt{a_n} - \sqrt{d_n})^2 + (\sqrt{b_n} - \sqrt{c_n})^2\right] \\ &\leq \frac{1}{2}\left(\sqrt{a_n} - \sqrt{d_n}\right)^2 \\ &= \frac{1}{2}\left(\frac{a_n - d_n}{\sqrt{a_n} + \sqrt{d_n}}\right)^2 \\ &\leq \frac{1}{2}\left(\frac{a_n - d_n}{2\sqrt{d_0}}\right)^2 \\ &= \frac{1}{8d_0}(a_n - d_n)^2 \ . \end{aligned}$$

Taking complex initial values, the same process produces uncountably many sequences due to choices in square roots. It turns out that the various choices can be studied using genus 2 theta functions. As in the genus 1 situation, the link comes from the doubling formulae of these functions (which can now be proved easily using Theorem 2.7):

Theorem 2.11. *Let $\Omega \in \mathbb{H}_2$. Then we have the following duplication formulae:*

$$\begin{aligned} \theta_0(2\Omega)^2 &= \frac{1}{4}\left(\theta_0(\Omega)^2 + \theta_1(\Omega)^2 + \theta_2(\Omega)^2 + \theta_3(\Omega)^2\right) \ , \\ \theta_1(2\Omega)^2 &= \frac{1}{2}\left(\theta_0(\Omega)\theta_1(\Omega) + \theta_2(\Omega)\theta_3(\Omega)\right) \ , \\ \theta_2(2\Omega)^2 &= \frac{1}{2}\left(\theta_0(\Omega)\theta_2(\Omega) + \theta_1(\Omega)\theta_3(\Omega)\right) \ , \\ \theta_3(2\Omega)^2 &= \frac{1}{2}\left(\theta_0(\Omega)\theta_3(\Omega) + \theta_1(\Omega)\theta_2(\Omega)\right) \ . \end{aligned}$$

This means that if one starts with the four numbers $\{\theta_0(\Omega), \theta_1(\Omega), \theta_2(\Omega), \theta_3(\Omega)\}$ for some $\Omega \in \mathbb{H}_2$, then it is possible to attain the numbers $\{\theta_0(2\Omega), \theta_1(2\Omega), \theta_2(2\Omega), \theta_3(2\Omega)\}$ via the four variable AGM. That is to say, this AGM is, as in genus 1, doubling the argument of theta functions. Define the following function $\Theta^{(n)} : \mathbb{H}_2 \to \mathbb{P}^3(\mathbb{C})$ by

$$\Theta^{(n)}(\Omega) = [\theta_0(\Omega)^n : \theta_1(\Omega)^n : \theta_2(\Omega)^n : \theta_3(\Omega)^n] \ .$$

At each stage there are eight possible choices (there are four choices of square roots to make, but taking an opposite set of signs gives the same result), and it turns out that they can be classified by the following (Proposition 3.10 in [Jar08])

Proposition 2.12. *Suppose $[a : b : c : d] \in \Theta^{(2)}(\Omega)$ for some $\Omega \in \mathbb{H}_2$. Then all possible results of the AGM map also lie in the image of $\Omega^{(2)}$. In particular, they all are of the form*

$$\Theta^{(2)}\left(\begin{pmatrix} I & 0 \\ C & I \end{pmatrix}(2\Omega)\right) \ ,$$

where I is the 2×2 identity matrix and C runs over the set

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \ .$$

Given a quadruple (a, b, c, d) such that there exists $\Omega \in \mathcal{F}^{(2)}$, the fundamental domain of $\mathbb{H}_2$, with $\Theta^{(2)}(\Omega) = [a : b : c : d]$, we say that $(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ is a *right choice* of square roots if $\Theta^{(1)}(\Omega) = [\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}]$. Similarly a *simplest value* is the value corresponding to a sequence where a right choice is taken at each step. Finally, denote by $\Gamma^{(2)}$ the group

$$\Gamma^{(2)} = \{\gamma \in \mathrm{Sp}_4(\mathbb{Z}) \mid \Theta^2(\gamma\Omega) = \Theta^{(2)}(\Omega) \text{ for all } \Omega \in \mathbb{H}_2\} \ ,$$

which is essentially the analogue of the principal subgroup for the standard upper half plane. Under these notations, we have the following (near) generalisation of the theorem of Gauss (Theorem 3.14 in [Jar08]):

Theorem 2.13. *For almost all quadruples (a, b, c, d), there exists $\Omega \in \mathbb{H}_2$ such that the good values of the AGM are precisely the values of the set*

$$\left\{ \frac{a}{\theta_0^2(M(\Omega))} \;\middle|\; M \in \Gamma^{(2)} \right\} \ .$$

Furthermore, the simplest values of the AGM are those of maximum modulus.

We demonstrate one example of how this four variable AGM can be useful in the computation of the determinant of the period matrix over $\mathbb{R}$. This is the work of [SvS12]. Consider the four partitions of branch points $S = \{1,3,5\}, \{1,4,5\}, \{2,3,5\}$ and $\{2,4,5\}$. Under the correspondence between partitions and theta functions described earlier this chapter, these correspond to the four genus 2 theta functions θ_0, θ_1, θ_2 and θ_3 respectively. Therefore Thomae's theorem gives four corresponding equations:

$$\begin{aligned}
\theta_0^2(\Omega) &= \frac{4\det\Omega_1}{\pi^2}\sqrt{(a_3-a_1)(a_5-a_1)(a_5-a_3)(a_4-a_2)},\\
\theta_1^2(\Omega) &= \frac{4\det\Omega_1}{\pi^2}\sqrt{(a_4-a_1)(a_5-a_1)(a_5-a_4)(a_4-a_3)},\\
\theta_2^2(\Omega) &= \frac{4\det\Omega_1}{\pi^2}\sqrt{(a_3-a_2)(a_5-a_2)(a_5-a_3)(a_4-a_1)},\\
\theta_3^2(\Omega) &= \frac{4\det\Omega_1}{\pi^2}\sqrt{(a_4-a_2)(a_5-a_2)(a_5-a_4)(a_3-a_1)},
\end{aligned}$$

where the fourth roots of unity are eliminated by the ordering of the roots. But recall that the (four variable) AGM of the four theta functions on the left hand side is 1, since the AGM is equivalent to period doubling. Hence we have the following:

Proposition 2.14. *Let C be a genus 2 hyperelliptic curve over $\mathbb{R}$ with real roots $a_1,\dots,a_5$ in increasing order and denote the period matrix by $\Omega_1\mathbb{Z}^2+\Omega_2\mathbb{Z}^2$. Then the determinants of the Ω_i's are given by*

$$\begin{aligned}
\det\Omega_1 &= \frac{\pi^2}{4M_4(A_1,A_2,A_3,A_4)}\ ,\\
\det\Omega_2 &= -\frac{\pi^2}{4M_4(B_1,B_2,B_3,B_4)}\ ,
\end{aligned}$$

where

$$\begin{aligned}
A_1 &= \sqrt{(a_3-a_1)(a_5-a_1)(a_5-a_3)(a_4-a_2)}\ , & A_2 &= \sqrt{(a_4-a_1)(a_5-a_1)(a_5-a_4)(a_4-a_3)}\ ,\\
A_3 &= \sqrt{(a_3-a_2)(a_5-a_2)(a_5-a_3)(a_4-a_1)}\ , & A_4 &= \sqrt{(a_4-a_2)(a_5-a_2)(a_5-a_4)(a_3-a_1)}\ ,\\
B_1 &= \sqrt{(a_3-a_1)(a_5-a_1)(a_5-a_3)(a_4-a_2)}\ , & B_2 &= \sqrt{(a_3-a_1)(a_4-a_1)(a_4-a_3)(a_5-a_2)}\ ,\\
B_3 &= \sqrt{(a_2-a_1)(a_5-a_1)(a_5-a_2)(a_4-a_3)}\ , & B_4 &= \sqrt{(a_2-a_1)(a_4-a_1)(a_4-a_2)(a_5-a_3)}\ .
\end{aligned}$$

An analogous version of this proposition can be done for higher genera hyperelliptic curves.

2.5.2 The Six Variable AGM

The second generalisation, which takes six numbers instead of four, is found in Bost and Mestre's paper [BM88]. Historically the algorithm was first written down by Richelot, using some ingenious change of variables whose origin seemed mysterious. It was then re-interpreted by Konigsberger using, in modern language, isogenies between abelian surfaces. Finally, the algorithm described here is due to Humbert as part of his work on Kummer surfaces.

Let $a < b < c < d < e < f$ be six real numbers. We define, by induction, six sequences using the following algorithm:

- Set $a_0 = a$, $b_0 = b$, $c_0 = c$, $d_0 = d$, $e_0 = e$ and $f_0 = f$.
- Set $P_n = (x - a_n)(x - b_n)$, $Q_n = (x - c_n)(x - d_n)$ and $R_n = (x - e_n)(x - f_n)$.
- Set $U_n = Q_n'R_n - R_n'Q_n$, $V_n = R_n'P_n - P_n'R_n$ and $W_n = P_n'Q_n - Q_n'P_n$.
- Set a_{n+1}, b_{n+1}, c_{n+1}, d_{n+1}, e_{n+1} and f_{n+1} to be the roots of $U_nV_nW_n$ in increasing order, that is, we have $a_{n+1} < b_{n+1} < c_{n+1} < d_{n+1} < e_{n+1} < f_{n+1}$.

If $\{u_n, u_n'\}$, $\{v_n, v_n'\}$ and $\{w_n, w_n'\}$ are the roots of U_n, V_n and W_n respectively, solving the equations gives the chain of inequalities

$$a_n < v_n < w_n < b_n < c_n < w_n' < u_n < d_n < e_n < u_n' < v_n' < f_n \ .$$

So after relabelling the roots of $U_nV_nW_n$ appropriately, one obtains

$$\begin{aligned} a_n < a_{n+1} < b_{n+1} < b_n \ , \\ c_n < c_{n+1} < d_{n+1} < d_n \ , \\ e_n < e_{n+1} < f_{n+1} < f_n \ , \end{aligned}$$

which suggests that the sequences (a_n) and (b_n), (c_n) and (d_n), (e_n) and (f_n) converge to three common limits. In fact, one can further show that not only do they converge to three common limits, but this convergence is quadratic. This follows from the observation that

$$V_n'W_n - W_n'V_n = -2\Delta_k P \ ,$$

where Δ_k is the determinant of the matrix of coefficients of P_n, Q_n and R_n with respect to the basis $1, x, x^2$. Then taking discriminant of both sides implies that

$$4(v_n - w_n)(v_n - w'_n)(v'_n - w_n)(v'_n - w'_n) = (v_n + v'_n - w_n - w'_n)^2(a_n - b_n)^2 \ ,$$

and when combined with the inequalities above gives (the first line of)

$$\begin{aligned} b_{n+1} - a_{n+1} &< \frac{(b+f-a-c)^2}{4(c-b)(e-b)(e-d)}(b_n - a_n)^2 \ , \\ d_{n+1} - c_{n+1} &< \frac{(d+f-a-c)^2}{4(c-b)(f-b)(e-d)}(d_n - c_n)^2 \ , \\ f_{n+1} - e_{n+1} &< \frac{(d+f-a-e)^2}{4(c-b)(e-b)(e-d)}(f_n - e_n)^2 \ . \end{aligned}$$

We call the three limits the AGM of these six real numbers.

Starting with a hyperelliptic curve $C_0 : y^2 = (x-a_0)(x-b_0)\cdots(x-f_0)$ with real roots, by applying the AGM to the six roots of C_0, the AGM then produces a family of hyperelliptic curves defined by

$$C_n : T_n^2 y^2 = (x-a_n)(x-b_n)\cdots(x-f_n) = P_n(x)Q_n(x)R_n(x) \ ,$$

where

$$T_n = \prod_{k=0}^{n} \frac{2\sqrt{-\Delta_k}}{\sqrt{(c_k+d_k-a_k-b_k)(e_k+f_k-c_k-d_k)(e_k+f_k-a_k-b_k)}} \ .$$

The reason of introducing such a constant is simply to normalise the leading coefficients of the curves. The relationship between this AGM and period integrals of hyperelliptic curves is summarised by the observation, due to Richelot, that

$$\int_{a_n}^{b_n} \frac{S(x)dx}{\sqrt{|P_n(x)Q_n(x)R_n(x)|}} = 2\,t_n \int_{a_{n+1}}^{b_{n+1}} \frac{S(x)dx}{\sqrt{|P_{n+1}(x)Q_{n+1}(x)R_{n+1}(x)|}} \ ,$$

where $S(x)$ is any degree 1 polynomial and the constant t_n is the individual component of T_n, that is

$$t_n = \frac{\sqrt{-\Delta_n}}{\sqrt{(c_n+d_n-a_n-b_n)(e_n+f_n-c_n-d_n)(e_n+f_n-a_n-b_n)}} \ .$$

An 'elementary' proof of the result can be found in the appendix of [BM88]. Replacing the limits of integration one gets similar identities for the other period integrals, for example

$$\int_{b_n}^{c_n} \frac{S(x)dx}{\sqrt{|P_n(x)Q_n(x)R_n(x)|}} = t_n \int_{b_{n+1}}^{c_{n+1}} \frac{S(x)dx}{\sqrt{|P_{n+1}(x)Q_{n+1}(x)R_{n+1}(x)|}} ,$$

Essentially this gives information on how the period integrals behave. More explicitly, by setting

$$I_a = \int_a^b \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} ,$$

the identity implies that

$$I_a = \lim_{n\to\infty} \left[\left(\prod_{k=0}^{n-1} t_k \right) \int_{a_n}^{b_n} \frac{S(x)dx}{\sqrt{-P_nQ_nR_n}} \right] = \frac{\pi T S(\alpha)}{(\beta-\alpha)(\gamma-\alpha)} ,$$

where T is the product of the t_n's and α, β, γ are the AGM of a, b, c, d, e and f with $\alpha < \beta < \gamma$. The second equality follows from the observation that in the limit the sextic polynomial in the integrand becomes $(x-\alpha)^2(x-\beta)^2(x-\gamma)^2$ and thus the integral is the residue of the function at the simple pole α. This gives the following theorem

Theorem 2.15. *Let C be a hyperelliptic curve given by*

$$y^2 = (x-a)(x-b)(x-c)(x-d)(x-e)(x-f)$$

with $a < b < \cdots < f$. Apply the Bost-Mestre algorithm to (a, b, c, d, e, f). Then for any polynomial $S(x)$ of degree 1 or less, we have

$$\int_a^b \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \frac{\pi T S(\alpha)}{(\beta-\alpha)(\gamma-\alpha)} ,$$
$$\int_c^d \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \frac{\pi T S(\beta)}{(\beta-\alpha)(\gamma-\beta)} ,$$
$$\int_e^f \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \frac{\pi T S(\gamma)}{(\gamma-\alpha)(\gamma-\beta)} ,$$

where α, β and γ are the AGM of $a, b, \ldots, f$ and T is the products of the t_k's.

By applying some linear transformations, one can obtain expressions for the remaining integrals. For example, by letting

$$y(x) = \frac{1}{2x - a - b} \ ,$$

then one sees that

$$(x - a) = \frac{1}{2}\left(\frac{1}{y} - \frac{1}{y(a)}\right) = -\frac{1}{2yy(a)}(y - y(a)) \ .$$

Notice that if $a < b < c < d < e < f$, then after the transformation we have the inequality $y(a) < y(f) < y(e) < y(d) < y(c) < y(b)$. Hence combining everything we get

$$\int_b^c \frac{S(x)dx}{\sqrt{(x-a)\cdots(x-f)}} = 4\sqrt{y(a)\cdots y(f)} \int_{y(c)}^{y(b)} \frac{S\left(\frac{1}{2}\left(\frac{1}{y} + a + b\right)\right) ydy}{\sqrt{-(y - y(a))\cdots(y - y(f))}} \ ,$$

and a similar result holds for the other integral.

To explicitly relate it to the AGM as above, denote by $(\alpha', \beta', \gamma')$ the AGM of $y(a)$, $y(f)$, $y(e)$, $y(d)$, $y(c)$ and $y(b)$. Consider the first case when $S(x) \equiv 1$; in this case we get

$$\int_b^c \frac{dx}{\sqrt{(x-a)\cdots(x-f)}} = \frac{4\sqrt{y(a)\cdots y(f)}\pi T'\gamma'}{(\gamma' - \beta')(\gamma' - \alpha')}$$

and

$$\int_d^e \frac{dx}{\sqrt{(x-a)\cdots(x-f)}} = \frac{4\sqrt{y(a)\cdots y(f)}\pi T'\beta'}{(\gamma' - \beta')(\beta' - \alpha')} \ ,$$

where T' is the corresponding value of T for this AGM. Finally if $S(x) = x$, then after the change of variables it becomes

$$S(y) = \left(\frac{a+b}{2}\right) y + \frac{1}{2}$$

and thus

$$\int_b^c \frac{xdx}{\sqrt{(x-a)\cdots(x-f)}} = \frac{2\sqrt{y(a)\cdots y(f)}\pi T' \left((a+b)\gamma' + 1\right)}{(\gamma' - \beta')(\gamma' - \alpha')}$$

and

$$\int_d^e \frac{xdx}{\sqrt{(x-a)\cdots(x-f)}} = \frac{2\sqrt{y(a)\cdots y(f)}\pi T'((a+b)\beta'+1)}{(\gamma'-\beta')(\beta'-\alpha')} \ .$$

The actual periods are then simply the sum of these period integrals formed by studying the symplectic basis of the homology group. In this way one may obtain the period matrix of the hyperelliptic curve using the AGM.

The genus 1 AGM is equivalent to the construction of a tower of elliptic curves through a 2-isogeny; Bost and Mestre offer a geometric interpretation of this in their paper as well. For all $n \geq 1$, there is a *(2,2)-correspondence*, also known as *Richelot's isogeny*, between the curves $C_n(x,y)$ and $C_{n+1}(x',y')$. A $(2,2)$-correspondence is a multivalued map that takes a point on C_n and returns two points on C_{n+1} (or equivalently, a degree 2 divisor on C_{n+1}) with kernel isomorphic to V_4.

More explicitly, this correspondence Z over $C_n \times C_{n+1}$ is defined by the pair of equations

$$\begin{cases} 0 = P_n(x)U_n(x') + Q_n(x)V_n(x') \\ yy' = P_n(x)U_n(x')(x-x') \end{cases}$$

Let π_1 and π_2 be the restrictions of Z of the projections of $C_n \times C_{n+1}$ onto C_n and C_{n+1} respectively. From the maps

$$H^0(C_{n+1},\Omega^1) \xrightarrow{\pi_2^*} H^0(Z,\Omega^1) \xrightarrow{\pi_{1*}} H^0(C_n,\Omega^1) \ ,$$

where π_{1*} is the trace map and π_2^* is the inverse image map, we get an action on the space of differentials $\delta : \Omega^1(C_{n+1}) \to \Omega^1(C_n)$ via the composition $\pi_{1*} \circ \pi_2^*$. Note that π_{1*} is dual to π_1^* by Serre duality (see [Ser59]). Since this action is linear, for any polynomial of degree 0 or 1, this gives the equality of differentials

$$\delta\left(S(x')\frac{dx'}{y'}\right) = S(x)\frac{dx}{y}$$

which is a key ingredient of the proof of Theorem 2.15. The maps π_1 and π_2 can be used to construct a map f between the corresponding Jacobians by $f\left([\sum n_i P_i]\right) = \left[\sum n_i \pi_1 \pi_2^{-1} P_i\right]$. The AGM is then constructing a tower of abelian surfaces

$$\cdots \to J_{n+1} \xrightarrow{f_n} J_n \to \cdots \to J_1 \xrightarrow{f_0} J_0 \ ,$$

where J_n is the Jacobian of the curve C_n. As n tends to infinity, the curve C_n becomes C_∞ – a singular curve with equation $T^2y^2 = (x-\alpha)^2(x-\beta)^2(x-\gamma)^2$ with two rational components (by taking the positive and negative square roots of C_∞), where α, β and γ are the AGM of $a_0, b_0, \ldots, f_0$. The integral of the differential $S(x)\dfrac{dx}{y}$ along the contour (a_n, b_n) becomes the residue at $(\alpha, 0)$.

We end on a brief remark. The defining equations of the Richelot isogeny seem to suggest that it depends on the ordering of P, Q and R. Indeed, a pair of points on C_n may map to four different points on C_{n+1} depending on how P, Q and R are ordered. However, it turns out that these always define equivalent divisors inside J_{n+1}, so that the homomorphism $J_{n+1} \longrightarrow J_n$ is well-defined and independent of the ordering. More details can be found in Chapter 8 of [Smi05].

2.6 Hyperelliptic Curves over $\mathbb{C}$

The main difficulty in extending the algorithm to curves with complex coefficients is the fact that the algorithm relies on a natural way in ordering the roots at every stage of the AGM. While there is such a canonical way when the roots are real (namely in increasing order), this is not the case with the complex numbers. Nonetheless, by carefully mimicking the method in [BM88], it is possible to derive a similar algorithm to compute the periods. We first present the full algorithm before giving a proof afterwards, and we end the section with some related theoretical results on the properties of the AGM itself.

2.6.1 The Algorithm

We first define the complex AGM. Let $a, b, \ldots, f$ be six distinct complex numbers. We define, by induction, six sequences using the following algorithm:

Algorithm 2.16 (Complex AGM)**.**
Input: Six distinct complex numbers a, b, c, d, e and f.
Ouput: Three distinct complex numbers α, β and γ.

1. *Set B_0 to be one of the initial numbers that has the smallest imaginary part and r_0 the minimal distance between the other five numbers and B_0. That is,*

$$B_0 \in \{a, b, c, d, e, f\}$$

such that

$$\operatorname{Im} B_0 = \min\{\operatorname{Im} a, \operatorname{Im} b, \ldots, \operatorname{Im} f\} \ ,$$

and

$$r_0 = \min\{|x - B_0| : x \in \{a, b, c, d, e, f\} \setminus \{B_0\}\} \ .$$

If two of the starting numbers have the same minimal imaginary parts, then let B_0 be the point with the smaller real part.

2. *Set the base point* $B = B_0 - \dfrac{2}{5} r_0$.

3. *Set a_0, b_0, c_0, d_0, e_0 and f_0 to be a permutation of the initial numbers, ordered by argument with respect to the base point B. That is, compute* $\arg(B - x) \in (-\pi, \pi]$ *for $x \in \{a, b, c, d, e, f\}$ and sort the numbers in increasing order.*

4. *Set, for $n \geq 0$,*

$$P_n = (x - a_n)(x - b_n) \ , \quad Q_n = (x - c_n)(x - d_n) \quad \text{and} \quad R_n = (x - e_n)(x - f_n) \ .$$

5. *Set*

$$\begin{aligned} U_n &= Q_n' R_n - R_n' Q_n = \varepsilon_1 (x - u_n)(x - u_n') \ , \\ V_n &= R_n' P_n - P_n' R_n = \varepsilon_2 (x - v_n)(x - v_n') \ , \\ W_n &= P_n' Q_n - Q_n' P_n = \varepsilon_3 (x - w_n)(x - w_n') \ . \end{aligned}$$

6. *Using the roots of U_n, V_n and W_n, form*

   - $P_{n+1} = (x - a_{n+1})(x - b_{n+1})$ *with* $a_{n+1} = v_n$ *and* $b_{n+1} = w_n$*;*
   - $Q_{n+1} = (x - c_{n+1})(x - d_{n+1})$ *with* $c_{n+1} = w_n'$ *and* $d_{n+1} = u_n$*;*
   - $R_{n+1} = (x - e_{n+1})(x - f_{n+1})$ *with* $e_{n+1} = u_n'$ *and* $f_{n+1} = v_n'$.

   The roots are picked so that the value of

$$|a_{n+1} - b_{n+1}| + |c_{n+1} - d_{n+1}| + |e_{n+1} - f_{n+1}|$$

   is minimal amongst the eight possible choices. If there exist two permutations with the same minimal distance, choose the one with the minimal angles between the roots.

7. *Repeat Steps 4 to 6 until the roots coincide to desired precision.*

The only difference between this and the algorithm for real numbers is how the sextuples $\{a_n, b_n, \ldots, f_n\}$ are ordered at each stage, and we provide some justification behind our choices. The first step proves to be the most troublesome, as there are 15 possible ways to order the roots. The method presented here (Steps 1 to 3) is identical to how Maple treats the Weierstrass points in computing the monodromy group of the algebraic covering (see [DvH99]). The base point B is essentially picked so that it is directly left of the left-most initial number, since it is advantageous for numerical accuracy to keep some distance from the Weierstrass points. The $\frac{2}{5}$ used to compute r_0 is somewhat arbitrary; any numbers between 0 and $\frac{1}{2}$ can be used.

After the first step, at each iteration we only get eight different ways to arrange the roots, coming from the two choices of roots for each of U_n, V_n and W_n in Step 5. Our right choice (i.e. picking the minimal distance between the roots) was motivated by two reasons. The first being that it is clearly compatible with Bost and Mestre's algorithm if the initial numbers are real, and the second is that this ensures that the algorithm converges to three (distinct) complex numbers quadratically. More explicitly, as in the real case, for each right choice made we have

$$\begin{aligned}
|a_{n+1} - b_{n+1}| &< \left| \frac{(b+f-a-c)^2}{4(c-b)(e-b)(e-d)} \right| |a_n - b_n|^2 \ , \\
|c_{n+1} - d_{n+1}| &< \left| \frac{(d+f-a-c)^2}{4(c-b)(f-b)(e-d)} \right| |c_n - d_n|^2 \ , \\
|e_{n+1} - f_{n+1}| &< \left| \frac{(d+f-a-e)^2}{4(c-b)(e-b)(e-d)} \right| |e_n - f_n|^2 \ .
\end{aligned}$$

Once we have a good notion of the complex AGM, the rest follows as in the real case: as one applies the AGM, we get the same identity (now as complex integrals, taken as the straight line between the end points)

$$\int_{a_n}^{b_n} \frac{S(x)dx}{\sqrt{P_n(x)Q_n(x)R_n(x)}} = 2\,t_n \int_{a_{n+1}}^{b_{n+1}} \frac{S(x)dx}{\sqrt{P_{n+1}(x)Q_{n+1}(x)R_{n+1}(x)}} \ ,$$

where t_n is defined as before (the branch of the square root is arbitrarily chosen in practice as explained later). One might remark that making the right choice at each stage guarantees that the three paths (the other two being from c_n to d_n and from e_n to f_n) do not cross. As n tends to infinity, we get

Proposition 2.17. *Let $C : y^2 = (x-a)(x-b)\cdots(x-f)$ be a hyperelliptic curve and α, β and γ be the AGM of $a, b, \ldots, f$. Then we have*

$$I_a(S(x)) = \int_a^b \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \pm\frac{\pi T S(\alpha)}{(\beta-\alpha)(\gamma-\alpha)} ,$$

$$I_c(S(x)) = \int_c^d \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \pm\frac{\pi T S(\beta)}{(\beta-\alpha)(\gamma-\beta)} ,$$

$$I_e(S(x)) = \int_e^f \frac{S(x)dx}{\sqrt{-(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \pm\frac{\pi T S(\gamma)}{(\gamma-\alpha)(\gamma-\beta)} ,$$

where $S(x)$ is any polynomial of degree 0 or 1 and T is defined as before.

There are some hidden subtleties here. Firstly, the natural ordering of real numbers led to a natural ordering of the three resulting numbers of the AGM (namely that $\alpha < \beta < \gamma$). But here we lack such ordering, so by saying that α, β and γ are the AGM of $a, b, \ldots, f$, we mean that in the limit we have

$$P(x) = (x-\alpha)^2 , \quad Q(x) = (x-\beta)^2 \quad \text{and} \quad R(x) = (x-\gamma)^2 .$$

The ambiguity of the sign on the right hand sides comes from the freedom to interchange a and b (and similarly the other two pairs of roots). But consider the loop that circles all three branch cuts on $\mathbb{P}^1(\mathbb{C})$, which can be contracted to a single point on the other side of the Riemann surface. This gives the identity $I_a(S(x)) - I_c(S(x)) + I_e(S(x)) = 0$ and one can easily deduce the correct signs by running through all four possibilities. Technically there are eight permutations but half of them are simply the negatives of the other half so the signs are only determined relative to one another; choosing the wrong set of signs ultimately gives a equivalent period matrix so it does not affect the outcome. This ambiguity also means that there is no need to distinguish the branch of square root used in the computation of t_n.

To compute the periods we also require the integrals between the remaining roots, that is, the integral of $S(x)\frac{dx}{y}$ from b to c and from d to e. But in this situation it turns out the lack of ordering becomes an advantage. A change of variable was required to satisfy a particular ordering of the roots in the real case, but here one can simply shift the order of the initial roots $a, b, \ldots, f$ and then reapply the same AGM process as above. More precisely, let

$a_0 = a$, $b_0 = f$, $c_0 = e$, $d_0 = d$, $e_0 = c$, $f_0 = b$. In this case the integral between b and c become the integral between e_0 and f_0, which we already know by the above proposition and hence:

$$I_b(S(x)) = \int_b^c \frac{S(x)dx}{\sqrt{(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \pm\frac{\pi T' S(\alpha')}{(\gamma'-\beta')(\gamma'-\alpha')} ,$$

$$I_d(S(x)) = \int_d^e \frac{S(x)dx}{\sqrt{(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \pm\frac{\pi T' S(\beta')}{(\beta'-\alpha')(\gamma'-\beta')} ,$$

where α', β', γ' and T' are from the associated AGM. Finally, from the standard symplectic basis we see that the period matrices are given by

$$\Omega_1 = \begin{pmatrix} I_a(1) & I_c(1) \\ I_a(x) & I_c(x) \end{pmatrix} \text{ and } \Omega_2 = \begin{pmatrix} I_b(1) + I_d(1) & I_d(1) \\ I_b(x) + I_d(x) & I_d(x) \end{pmatrix} .$$

The same subtlety occurs here in the computations of $I_b(S(x))$ and $I_d(S(x))$. In practice the easiest solution to determining all the correct signs is simply to insist that the matrix $\Omega_1^{-1}\Omega_2$ is symmetric with a positive definite imaginary part by running through all possible permutations (in practice this is not too bad; the Magma codes in Appendix A compute the period matrix to 500 decimal places in under 5 seconds).

Here we have not studied in great detail the situation when one makes the wrong choice, though through numerical evidence and our understanding of the Richelot isogeny it would appear that in practice some of these choices do not matter. Since the algorithm boils down to the equality of some complex integrals (see Proposition 2.19 in the next subsection), this holds true even if the wrong choice is made and a different hyperelliptic curve is obtained. The Richelot isogeny is a well-defined map between the Jacobians regardless of how the roots are labelled. All information regarding how the period integrals behave under the correspondence is, therefore, simply stored inside the t_n's and in the limit these give the same answers.

Combining everything we obtain:

Algorithm 2.18 (Computing the period matrix of a hyperelliptic curve)**.**
Input: A genus 2 hyperelliptic curve C over $\mathbb{C}$ defined by the equation

$$y^2 = (x-a)(x-b)(x-c)(x-d)(x-e)(x-f) \ .$$

Ouput: Big period matrix $\Omega = \begin{pmatrix} \Omega_1 & \Omega_2 \end{pmatrix}$ of C.

1. *Set $a_0 = a$, $b_0 = b$, $c_0 = c$, $d_0 = d$, $e_0 = e$ and $f_0 = f$ (ordered as in Algorithm 2.16) and apply the AGM to $a_0, \ldots, f_0$ to obtain three limits α, β and γ.*

2. *Compute the three period integrals*

$$I_a = \frac{\pi TS(\alpha)}{(\beta-\alpha)(\gamma-\alpha)}, \quad I_c = \pm\frac{\pi TS(\beta)}{(\beta-\alpha)(\gamma-\beta)}, \quad \text{and} \quad I_e = \pm\frac{\pi TS(\gamma)}{(\gamma-\alpha)(\gamma-\beta)}$$

   for both $S(x) \equiv 1$ and $S(x) = x$, where the signs are picked such that $I_a - I_c + I_e = 0$.

3. *Apply the AGM by setting $a_0 = a$, $b_0 = f$, $c_0 = e$, $d_0 = d$, $e_0 = c$, $f_0 = b$ and obtain, as in Step 2, three complex numbers, two of which must be I_b and I_d.*

4. *Form the matrices ω_1 and ω_2*

$$\Omega_1 = \begin{pmatrix} I_a(1) & I_c(1) \\ I_a(x) & I_c(x) \end{pmatrix} \text{ and } \Omega_2 = \begin{pmatrix} I_b(1) + I_d(1) & I_d(1) \\ I_b(x) + I_d(x) & I_d(x) \end{pmatrix} \ ,$$

   where I_b and I_d are two of the three outputs in Step 3, chosen by insisting that the matrix $\Omega_1^{-1}\Omega_2$ is a Riemann matrix.

5. *The period matrix is given by $\Omega = \begin{pmatrix} \Omega_1 & \Omega_2 \end{pmatrix}$.*

For example, suppose we take the curve

$$y^2 = (x-1)(x-i)(x-1-i)(x-1+i)(x+i)(x+1+i) \ .$$

Then using the Magma code in Appendix A, one obtains the following small period matrix

```
[0.30445405313965537307578186 2812 + 1.17042114161322302328979034220*i
    0.15524963038805160474084032 8807 + 0.47246609705093033850370935 4719*i]
[0.15524963038805160474084032 8810 + 0.47246609705093033850370935 4718*i
    0.30445405313965537307578186 2813 + 1.17042114161322302328979034220*i]
```

which agrees with the answer from the inbuilt Magma function (details on Magma's method can be found in [Wam06]).

2.6.2 Proof of the Algorithm

We now provide an elementary proof of Algorithm 2.18 over the complex numbers, following mostly the series of questions in the appendix of [BM88] (with slight modifications to account for complex numbers).

Let $a_0, b_0, \ldots, f_0$ be six distinct complex numbers, denote the sequences obtained from the right choice of the AGM by $\{a_n\}, \{b_n\}, \ldots, \{f_n\}$. Write the roots of U_n (V_n and W_n respectively) as u_n and u'_n (v_n and v'_n, w_n and w'_n respectively). Assume that the right choice pair together the roots (v, w), (w', u) and (u', v'). The link between the AGM and the computation of periods is the following observation, which we will now prove.

Proposition 2.19. *For all n, we have*

$$\int_{a_n}^{b_n} \frac{dx}{\sqrt{P_n(x)Q_n(x)R_n(x)}} = 2\sqrt{-\Delta_n} \int_{v_n}^{w_n} \frac{dx}{\sqrt{U_n(x)V_n(x)W_n(x)}} \ ,$$

where Δ_n is the determinant of the 3×3 matrix defined by the coefficients of P_n, Q_n and R_n.

Note that by interchanging the limits, one obtains various similar results with the same method. We drop the subscripts in the following for notational convenience. Define the following polynomial in two variables

$$F(x, z) = P(x)U(z) + Q(x)V(z) \ .$$

Note that we also have $F(x, z) = -R(x)W(z) - (x - z)^2\Delta$, following from the identity

$$P(x)U(z) + Q(x)V(z) + R(x)W(z) + (x - z)^2\Delta = 0$$

which one can check by direct computation. Rewriting $F(x, z) = \phi_0(x)z^2 + \phi_1(x)z + \phi_2(x)$ as a degree 2 polynomial in z, define z_1 and z_2 to be the roots of this polynomial. That is,

$$z_1(x) = \frac{-\phi_1(x) + \sqrt{\phi_1(x)^2 - 4\phi_0(x)\phi_2(x)}}{2\phi_0(x)} \ ,$$
$$z_2(x) = \frac{-\phi_1(x) - \sqrt{\phi_1(x)^2 - 4\phi_0(x)\phi_2(x)}}{2\phi_0(x)} \ .$$

Let us now study the functions z_i more carefully.

Lemma 2.20. *The functions $z_i(x)$ satisfy the following:*

(i) *They map the roots of $P(x)$ to the same point; that is*

$$z_1(a) = z_1(b) = v' \quad \textit{and} \quad z_2(a) = z_2(b) = v \ .$$

(ii) *There are fixed points at the roots of W; that is,*

$$z_1(w') = w' \quad \textit{and} \quad z_2(w) = w \ .$$

Proof. Since $F(a,z) = Q(a)V(z)$, we see that

$$\begin{aligned} \phi_0(a) &= Q(a)(e+f-a-b) \ , \\ \phi_1(a) &= 2Q(a)(ab-ef) \ , \\ (\phi_1^2 - 4\phi_0\phi_2)(a) &= \mathrm{disc}(Q(a)V(z)) = Q(a)^2\mathrm{disc}(V(z)) \ . \end{aligned}$$

From $0 = F(a, z_i(a)) = Q(a)V(z_i(a))$ and $Q(a) \neq 0$, it follows that $z_1(a)$ and $z_2(a)$ are both roots of V. The above calculation shows that $z_i(x)$ maps a to the different roots of V; for if $z_1(x) = z_2(x)$, then x must be a root of $\phi_1^2 - 4\phi_0\phi_2$. Doing the same calculations to b we see that

$$z_1(a) = \frac{-2ab + 2ef + \sqrt{\mathrm{disc}(V)}}{2(e+f-a-b)} = z_1(b) \ .$$

We conclude from this that $z_i(x)$ maps the two roots of $P(x)$ to the same point. Similarly we also have

$$z_1(c) = z_1(d) = u' \quad \text{and} \quad z_2(c) = z_2(d) = u \ .$$

Finally, assume that $z_1(x) = x$ (which implies $x \neq c$ or d from the above). From the identity $R(x)W(z_i(x)) = 0$, we see that there are fixed points at w and w'. Since $z_i(x)$ are holomorphic functions around some neighbourhood of a and the right choice is made so that v and w are close together, we must have $z_2(w) = w$. □

Now define the following functions

$$y_1(x) = \frac{P(x)U(z_1(x))(x - z_1(x))}{\sqrt{P(x)Q(x)R(x)}} \quad \text{and} \quad y_2(x) = \frac{P(x)U(z_2(x))(x - z_2(x))}{\sqrt{P(x)Q(x)R(x)}} \ .$$

We now have a series of purely computational results.

Proposition 2.21. *The functions $y_1(x)$ and $y_2(x)$ satisfy*

$$y_1^2(x) = \frac{U(z_1(x))V(z_1(x))W(z_1(x))}{\Delta} \quad \text{and} \quad y_2^2(x) = \frac{U(z_2(x))V(z_2(x))W(z_2(x))}{\Delta} \ .$$

Proof. Since $F(x, z_1(x)) = 0$ for all x, direct computation shows that

$$\begin{aligned} y_1^2(x) &= \frac{P(x)^2U(z_1(x))^2(x - z_1(x))^2}{P(x)Q(x)R(x)} \\ &= -\frac{P(x)U(z_1(x))Q(x)V(z_1(x))(x - z_1(x))^2\Delta}{P(x)Q(x)R(x)\Delta} \\ &= \frac{P(x)U(z_1(x))Q(x)V(z_1(x))R(x)W(z_1(x))}{P(x)Q(x)R(x)\Delta} \\ &= \frac{U(z_1(x))V(z_1(x))W(z_1(x))}{\Delta} \end{aligned}$$

and similarly for $y_2(x)$. □

This shows that the two maps $(x, y) \mapsto (z_i(x), y_i(x))$ are maps of hyperelliptic curves from C to C', where C and C' are defined through the equations $y^2 = P(x)Q(x)R(x)$ and $\Delta y^2 = U(x)V(x)W(x)$ respectively. Therefore together they define a $(2, 2)$-correspondence by sending the point (x, y) to the divisor $[(z_1(x), y_1(x)) + (z_2(x), y_2(x))]$.

Lemma 2.22. *We have*

$$U'(z_1(x))\frac{z_1'(x)}{y_1(x)} + U'(z_2(x))\frac{z_2'(x)}{y_2(x)} = -\frac{U'(x)}{\sqrt{P(x)Q(x)R(x)}}$$

and

$$V'(z_1(x))\frac{z_1'(x)}{y_1(x)} + V'(z_2(x))\frac{z_2'(x)}{y_2(x)} = -\frac{V'(x)}{\sqrt{P(x)Q(x)R(x)}} \ .$$

Proof. Again we directly compute that

$$\begin{aligned} &U'(z_1(x))\frac{z_1'(x)}{y_1(x)} + U'(z_2(x))\frac{z_2'(x)}{y_2(x)} \\ &= \frac{\sqrt{P(x)Q(x)R(x)}}{P(x)}\left(\frac{U'(z_1(x))z_1'(x)}{U(z_1(x))(x - z_1(x))} + \frac{U'(z_2(x))z_2'(x)}{U(z_2(x))(x - z_2(x))}\right) \\ &= -\frac{\sqrt{P(x)Q(x)R(x)}}{P(x)}\left(\frac{U'(x)}{Q(x)R(x)}\right) \\ &= -\frac{U'(x)}{\sqrt{P(x)Q(x)R(x)}} \end{aligned}$$

(the second equality was simplified with the help of Maple). □

Proposition 2.23. *We have*

$$\frac{z_1'(x)}{y_1(x)} + \frac{z_2'(x)}{y_2(x)} = -\frac{1}{\sqrt{P(x)Q(x)R(x)}} \ .$$

Proof. One can view the equations in the last lemma as a linear system of equations in the variables $\dfrac{z_i'(x)}{y_i(x)}$. Solving these equations give

$$\begin{aligned}
\frac{z_1'(x)}{y_1(x)} &= \frac{1}{\sqrt{P(x)Q(x)R(x)}} \left(\frac{V'(z_2(x))U'(x) - U'(z_2(x))V'(x)}{U'(z_1(x))V'(z_2(x)) - U'(z_2(x))V'(z_1(x))} \right) \ , \\
\frac{z_2'(x)}{y_2(x)} &= \frac{1}{\sqrt{P(x)Q(x)R(x)}} \left(\frac{U'(z_1(x))V'(x) - V'(z_1(x))U'(x)}{U'(z_1(x))V'(z_2(x)) - U'(z_2(x))V'(z_1(x))} \right) \ .
\end{aligned}$$

We proceed by computing each term. Let

$$U(x) = u_2x^2 + u_1x + u_0 \quad \text{and} \quad V(x) = v_2x^2 + v_1x + v_0 \ .$$

Then we have

$$V'(x)U'(y) - U'(x)V'(y) = 2(u_1v_2 - u_2v_1)(x - y) \ .$$

Plugging in the corresponding values give

$$\begin{aligned}
V'(z_2(x))U'(x) - U'(z_2(x))V'(x) &= 2(u_1v_2 - u_2v_1)(z_2(x) - x) \ , \\
U'(z_1(x))V'(x) - V'(z_1(x))U'(x) &= 2(u_2v_1 - u_1v_2)(z_1(x) - x) \ , \\
U'(z_1(x))V'(z_2(x)) - V'(z_1(x))U'(z_2(x)) &= 2(u_2v_1 - u_1v_2)(z_1(x) - z_2(x)) \ .
\end{aligned}$$

Since

$$\frac{2(u_1v_2 - u_2v_1)(z_2(x) - x) + 2(u_2v_1 - u_1v_2)(z_1(x) - x)}{2(u_2v_1 - u_1v_2)(z_1(x) - z_2(x))} = 1 \ ,$$

we conclude that

$$\frac{z_1'(x)}{y_1(x)} + \frac{z_2'(x)}{y_2(x)} = -\frac{1}{\sqrt{P(x)Q(x)R(x)}}$$

as required. □

Equivalently the proposition gives

$$\frac{dz_1(x)}{y_1(x)} + \frac{dz_2(x)}{y_2(x)} = -\frac{dx}{\sqrt{P(x)Q(x)R(x)}}$$

and hence

$$\int_a^b \frac{dx}{\sqrt{P(x)Q(x)R(x)}} = -\int_a^b \frac{dz_1(x)}{y_1(x)} - \int_a^b \frac{dz_2(x)}{y_2(x)} \ .$$

It remains to show that the limits are mapped to the corresponding points under the change of variables. The first integral vanishes since the integrand is holomorphic on some simply connected open subset of $\mathbb{C}$ near the point v', whence

$$\int_a^b \frac{dz_1(x)}{y_1(x)} = \sqrt{-\Delta} \oint_\gamma \frac{dx}{\sqrt{U(x)V(x)W(x)}} = 0 \ ,$$

where γ is a closed loop starting at the point v' which contains no singular points.

For the second integral notice that $y_2(x)$ has a zero at w, which is near v. Hence the path from a to b is mapped onto a closed path γ' starting at v, goes through w before looping back to v. This means γ' passes to the other covering of $\mathbb{C} \cup \{\infty\}$ and thus adds a minus sign when integrating back from w to v. This implies that

$$\int_a^b \frac{dz_2(x)}{y_2(x)} = -\sqrt{-\Delta} \oint_{\gamma'} \frac{dx}{\sqrt{U(x)V(x)W(x)}} = -2\sqrt{-\Delta} \int_v^w \frac{dx}{\sqrt{U(x)V(x)W(x)}}$$

which proves Proposition 2.19:

$$\int_{a_n}^{b_n} \frac{dx}{\sqrt{P_n(x)Q_n(x)R_n(x)}} = 2\sqrt{-\Delta_n} \int_{v_n}^{w_n} \frac{dx}{\sqrt{U_n(x)V_n(x)W_n(x)}} \ .$$

It follows that

Theorem 2.24. *We have*

$$I_a(S(x)) = \int_a^b \frac{S(x)dx}{\sqrt{(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)}} = \frac{\pi T S(\alpha)}{(\beta-\alpha)(\gamma-\alpha)} \ ,$$

where $S(x)$ is any degree 1 polynomial and $T = \prod_{n\geq 1} 2\,t_n$ with

$$t_n = \frac{\sqrt{-\Delta_n}}{\sqrt{(c_n+d_n-a_n-b_n)(e_n+f_n-c_n-d_n)(e_n+f_n-a_n-b_n)}} \ .$$

Proof. The required integral is given by

$$I_a(S(x)) = \lim_{n\to\infty} \left[\left(\prod_{k=0}^{n-1} 2\, t_k \right) \int_{a_n}^{b_n} \frac{S(x)dx}{\sqrt{P_n Q_n R_n}} \right] .$$

Note that for simplicity we assumed $S(x) \equiv 1$ in the previous calculations. Firstly, since the t_n's are the ratio between successive integrals, their convergence is automatic if the limit of the integrals exists. Now because the right choices are made in the AGM, the six initial numbers converge to three pairs and the curve $C_n : T_n^2 y^2 = P_n Q_n R_n$ tends to the singular curve

$$T^2 y^2 = (x-\alpha)^2 (x-\beta)^2 (x-\gamma)^2 .$$

Thus the integrand has a simple pole at α and in the limits the integral becomes the contour along the cycle surrounding a_n and b_n and is equal to the residue at the simple pole α, which gives the result. □

2.6.3 An Algebraic Interpretation

The Bost-Mestre algorithm can be viewed as a $(2,2)$-correspondence from a geometric standpoint as discussed before. But in the closing of this chapter we show directly, from a more algebraic approach using theta functions, that the algorithm is equivalent to doubling the period matrix of the hyperelliptic curve (which we saw in the genus 1 case).

Any sextic model of a genus 2 curve C can be reduced to a quintic by sending one of the roots to infinity. Furthermore, taking the cross ratio of $(x, a_1; a_0, a_\infty)$, with a_0, a_1 and a_∞ roots of the sextic, gives a transformation

$$x' = \frac{x-a_0}{x-a_\infty} \cdot \frac{a_1 - a_\infty}{a_1 - a_0}$$

which turns in the original sextic into a quintic of the form

$$y'^2 = x'(x'-1)(x'-\lambda)(x'-\mu)(x'-\nu) .$$

That is, a_0 is sent to 0, a_1 is sent to 1 and a_∞ is sent to infinity. We say that a curve of this form is in *Rosenhain (normal) form*. Then given such a curve, Corollary 2.10 immediately gives that

$$\lambda = \left(\frac{\theta_0(\Omega)\theta_9(\Omega)}{\theta_5(\Omega)\theta_7(\Omega)}\right)^2 , \quad \mu = \left(\frac{\theta_1(\Omega)\theta_9(\Omega)}{\theta_5(\Omega)\theta_6(\Omega)}\right)^2 \quad \text{and} \quad \nu = \left(\frac{\theta_0(\Omega)\theta_1(\Omega)}{\theta_6(\Omega)\theta_7(\Omega)}\right)^2 .$$

We note that these are different from the standard equations one might find in literature, though they define isomorphic curves. The discrepancy arose from a different ordering of roots – here we numbered the a_i with $\{0, 1, \lambda, \mu, \nu\}$ whereas most literature uses the numbering $\{\lambda, \mu, \nu, 0, 1\}$. One of the reasons for this ordering is due to the fact that this coincides with the choice Magma makes, which made some numerical computations more convenient. We briefly state the relevant duplication formulae which we employ later:

Corollary 2.25. *We have*

$$\begin{aligned}
\theta_0(2\Omega)^2 &= \frac{1}{4}\left(\theta_0(\Omega)^2 + \theta_1(\Omega)^2 + \theta_2(\Omega)^2 + \theta_3(\Omega)^2\right) , \\
\theta_5(2\Omega)^2 &= \frac{1}{4}\left(\theta_0(\Omega)^2 - \theta_1(\Omega)^2 - \theta_2(\Omega)^2 + \theta_3(\Omega)^2\right) , \\
\theta_7(2\Omega)^2 &= \frac{1}{4}\left(\theta_0(\Omega)^2 + \theta_1(\Omega)^2 - \theta_2(\Omega)^2 - \theta_3(\Omega)^2\right) , \\
\theta_9(2\Omega)^2 &= \frac{1}{4}\left(\theta_0(\Omega)^2 - \theta_1(\Omega)^2 + \theta_2(\Omega)^2 - \theta_3(\Omega)^2\right) .
\end{aligned}$$

This is another direct application of Theorem 2.7. The next set of identities comes from the Frobenius' theta formula. These are by no means the only theta identities (see the appendix of [Gau07] for a slightly more comprehensive list), but merely the ones which we employ in the later proofs.

Corollary 2.26. *We have the following identities.*

$$\begin{aligned}
\theta_2(\Omega)^2\theta_3(\Omega)^2 &= \theta_0(\Omega)^2\theta_1(\Omega)^2 - \theta_6(\Omega)^2\theta_7(\Omega)^2 , \\
\theta_3(\Omega)^2\theta_8(\Omega)^2 &= \theta_1(\Omega)^2\theta_9(\Omega)^2 - \theta_5(\Omega)^2\theta_6(\Omega)^2 , \\
\theta_2(\Omega)^2\theta_8(\Omega)^2 &= \theta_0(\Omega)^2\theta_9(\Omega)^2 - \theta_5(\Omega)^2\theta_7(\Omega)^2 , \\
\theta_3(\Omega)^2\theta_4(\Omega)^2 &= \theta_0(\Omega)^2\theta_5(\Omega)^2 - \theta_7(\Omega)^2\theta_9(\Omega)^2 , \\
\theta_0(\Omega)^2\theta_8(\Omega)^2 &= \theta_2(\Omega)^2\theta_9(\Omega)^2 - \theta_4(\Omega)^2\theta_6(\Omega)^2 , \\
\theta_8(\Omega)^2\theta_9(\Omega)^2 &= \theta_0(\Omega)^2\theta_2(\Omega)^2 - \theta_1(\Omega)^2\theta_3(\Omega)^2 , \\
\theta_8(\Omega)^4 + \theta_9(\Omega)^4 &= \theta_0(\Omega)^4 + \theta_1(\Omega)^4 - \theta_2(\Omega)^4 \ - \theta_3(\Omega)^4 .
\end{aligned}$$

Proof. The proofs of these identities are obtained by plugging in the correct values into Proposition 2.8; we only prove the last one here. Let $\mathbf{z}_i = \mathbf{0}$ for $1 \leq i \leq 4$. Then setting

$$\mathbf{a}_i = \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

for $1 \leq i \leq 4$ gives the two identities

$$\begin{aligned} -\theta_0(\Omega)^4 + \theta_3(\Omega)^4 + \theta_7(\Omega)^4 + \theta_8(\Omega)^4 &= 0 \\ \theta_1(\Omega)^4 - \theta_2(\Omega)^4 - \theta_7(\Omega)^4 + \theta_9(\Omega)^4 &= 0 \end{aligned}$$

respectively (since odd theta functions vanish at $\mathbf{z} = \mathbf{0}$). Combining these give the desired result. □

We are now ready to prove the theorem:

Theorem 2.27. *Let C be a hyperelliptic curve in Rosenhain form, given by the equation*

$$C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

with λ, μ and ν distinct complex numbers and denote the period matrix of C by $\Omega \in \mathbb{H}_2$. Apply the Bost-Mestre arithmetic-geometric mean to C and denote the resulting curve by C'. Then the period matrix of C' is given by 2Ω. More precisely, C' can reduced to Rosenhain form

$$C' : y^2 = x(x-1)(x-\lambda')(x-\mu')(x-\nu')$$

such that

$$\lambda' = \left(\frac{\theta_0(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_7(2\Omega)}\right)^2 , \quad \mu' = \left(\frac{\theta_1(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_6(2\Omega)}\right)^2 \quad \textit{and} \quad \nu' = \left(\frac{\theta_0(2\Omega)\theta_1(2\Omega)}{\theta_6(2\Omega)\theta_7(2\Omega)}\right)^2 .$$

Proof. Apply the Bost-Mestre algorithm to five roots of C by letting

$$P = x(x-1) , \quad Q = (x-\lambda)(x-\mu) , \quad \text{and} \quad R = x - \nu .$$

Therefore the equation of C' is given by

$$C' : y^2 = (x-a)(x-b)(x-c)(x-d)(x-e)(x-f) ,$$

where

$$\begin{aligned}
a &= \nu - \sqrt{\nu^2 - \nu}\ , \\
b &= \frac{\lambda\mu - \sqrt{\lambda\mu(\lambda-1)(\mu-1)}}{\lambda+\mu-1}\ , \\
c &= \frac{\lambda\mu + \sqrt{\lambda\mu(\lambda-1)(\mu-1)}}{\lambda+\mu-1}\ , \\
d &= \nu - \sqrt{(\mu-\nu)(\lambda-\nu)}\ , \\
e &= \nu + \sqrt{(\mu-\nu)(\lambda-\nu)}\ , \\
f &= \nu + \sqrt{\nu^2 - \nu}\ .
\end{aligned}$$

To transform C' into Rosenhain form, we take the transformation

$$x' = \frac{x-a}{x-f} \cdot \frac{b-f}{b-a}$$

or

$$x = \frac{(b-a)fx' - (b-f)a}{(b-a)x' - (b-f)}\ ,$$

which gives

$$C' : y'^2 = x'(x'-1)\left(x' - \frac{(b-f)(a-c)}{(c-f)(a-b)}\right)\left(x' - \frac{(b-f)(a-d)}{(d-f)(a-b)}\right)\left(x' - \frac{(b-f)(a-e)}{(e-f)(a-b)}\right)\ .$$

It suffices to show that

$$\frac{(b-f)(a-c)}{(c-f)(a-b)} = \left(\frac{\theta_0(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_7(2\Omega)}\right)^2\ , \tag{2.1}$$

$$\frac{(b-f)(a-d)}{(d-f)(a-b)} = \left(\frac{\theta_1(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_6(2\Omega)}\right)^2\ , \tag{2.2}$$

$$\frac{(b-f)(a-e)}{(e-f)(a-b)} = \left(\frac{\theta_0(2\Omega)\theta_1(2\Omega)}{\theta_6(2\Omega)\theta_7(2\Omega)}\right)^2\ . \tag{2.3}$$

This amounts to some elementary but tedious manipulation of theta functions. We start with the first case.

On the right hand side, following from the formulae in Corollary 2.25 and Corollary 2.26 one has

$$\begin{aligned}\left(\frac{\theta_0(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_7(2\Omega)}\right)^2 &= \frac{(\theta_0^2-\theta_1^2+\theta_2^2-\theta_3^2)(\theta_0^2+\theta_1^2+\theta_2^2+\theta_3^2)}{(\theta_0^2-\theta_1^2-\theta_2^2+\theta_3^2)(\theta_0^2+\theta_1^2-\theta_2^2-\theta_3^2)}\\ &= 1+\frac{4(\theta_0^2\theta_2^2-\theta_1^2\theta_3^2)}{[\theta_0^4-\theta_1^4+\theta_2^4-\theta_3^4]-2[\theta_0^2\theta_2^2-\theta_1^2\theta_3^2]}\\ &= 1+\frac{4\theta_8^2\theta_9^2}{\theta_8^4+\theta_9^4-2\theta_8^2\theta_9^2}\\ &= \left(\frac{\theta_9^2+\theta_8^2}{\theta_9^2-\theta_8^2}\right)^2\end{aligned}$$

Note that here $\theta_i = \theta_i(\Omega)$ for convenience. We try to indicate which formulae were used by the square brackets. And on the left hand side we have

$$\begin{aligned}\frac{(b-f)(a-c)}{(c-f)(a-b)} &= \frac{2\lambda\mu\nu-\lambda\mu-\lambda\nu-\mu\nu+\nu+2\sqrt{\lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1)}}{2\lambda\mu\nu-\lambda\mu-\lambda\nu-\mu\nu+\nu-2\sqrt{\lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1)}}\\ &= \left(\frac{2\lambda\mu\nu-\lambda\mu-\lambda\nu-\mu\nu+\nu+2\sqrt{\lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1)}}{\lambda\mu-\lambda\nu-\mu\nu+\nu}\right)^2\\ &= \left(1+\frac{2\lambda\mu(\nu-1)+2\sqrt{\lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1)}}{\lambda\mu-\lambda\nu-\mu\nu+\nu}\right)^2 .\end{aligned}$$

After substituting

$$\lambda = \left(\frac{\theta_0(\Omega)\theta_9(\Omega)}{\theta_5(\Omega)\theta_7(\Omega)}\right)^2 , \quad \mu = \left(\frac{\theta_1(\Omega)\theta_9(\Omega)}{\theta_5(\Omega)\theta_6(\Omega)}\right)^2 \quad \text{and} \quad \nu = \left(\frac{\theta_0(\Omega)\theta_1(\Omega)}{\theta_6(\Omega)\theta_7(\Omega)}\right)^2$$

into the above we get

$$\begin{aligned}\lambda\mu-\lambda\nu-\mu\nu+\nu &= \frac{\theta_0^2\theta_1^2([\theta_7^2\theta_9^2-\theta_0^2\theta_5^2]\theta_6^2\theta_9^2-[\theta_1^2\theta_9^2-\theta_5^2\theta_6^2]\theta_5^2\theta_7^2)}{\theta_5^4\theta_6^4\theta_7^4}\\ &= -\frac{\theta_0^2\theta_1^2\theta_3^2(\theta_4^2\theta_6^2\theta_9^2+\theta_5^2\theta_7^2\theta_8^2)}{\theta_5^4\theta_6^4\theta_7^4} ,\\ \lambda\mu(\nu-1) &= \frac{\theta_0^2\theta_1^2\theta_9^4[\theta_0^2\theta_1^2-\theta_6^2\theta_7^2]}{\theta_5^2\theta_6^2\theta_7^4} = \frac{\theta_0^2\theta_1^2\theta_2^2\theta_3^2\theta_9^4}{\theta_5^2\theta_6^2\theta_7^4} ,\\ \lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1) &= \frac{\theta_0^4\theta_1^4\theta_9^4[\theta_0^2\theta_1^2-\theta_6^2\theta_7^2][\theta_1^2\theta_9^2-\theta_5^2\theta_6^2][\theta_0^2\theta_9^2-\theta_5^2\theta_7^2]}{\theta_5^8\theta_6^8\theta_7^8}\\ &= \frac{\theta_0^4\theta_1^4\theta_2^4\theta_3^4\theta_8^4\theta_9^4}{\theta_5^8\theta_6^8\theta_7^8} .\end{aligned}$$

Therefore after much cancellation we have

$$\begin{aligned}\frac{(b-f)(a-c)}{(c-f)(a-b)} &= \left(1-\frac{2\theta_2^2\theta_9^4+2\theta_2^2\theta_8^2\theta_9^2}{\theta_4^2\theta_6^2\theta_9^2+\theta_5^2\theta_7^2\theta_8^2}\right)^2 \\ &= \left(1-\frac{2\theta_2^2\theta_9^4+2\theta_2^2\theta_8^2\theta_9^2}{[\theta_4^2\theta_6^2\theta_9^2+\theta_0^2\theta_8^2\theta_9^2]+[\theta_5^2\theta_7^2\theta_8^2-\theta_0^2\theta_8^2\theta_9^2]}\right)^2 \\ &= \left(1-\frac{2\theta_9^4+2\theta_8^2\theta_9^2}{\theta_9^4-\theta_8^4}\right)^2 \\ &= \left(\frac{\theta_9^2+\theta_8^2}{\theta_9^2-\theta_8^2}\right)^2\end{aligned}$$

which shows that

$$\frac{(b-f)(a-c)}{(c-f)(a-b)} = \left(\frac{\theta_0(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_7(2\Omega)}\right)^2$$

which proves (2.1). Unfortunately this was the neatest part in the sense that the expressions actually factorise nicely. For the second part we wish to show that

$$\frac{(b-f)(a-d)}{(d-f)(a-b)} = \left(\frac{\theta_1(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_6(2\Omega)}\right)^2 .$$

On the right hand side we have

$$\begin{aligned}\left(\frac{\theta_1(2\Omega)\theta_9(2\Omega)}{\theta_5(2\Omega)\theta_6(2\Omega)}\right)^2 &= 1+2\frac{(\theta_0\theta_3+\theta_1\theta_2)(\theta_0\theta_2+\theta_1\theta_3)}{(\theta_0^2-\theta_1^2-\theta_2^2+\theta_3^2)(\theta_0\theta_1-\theta_2\theta_3)} \\ &= 1+2\frac{\Theta_1}{\Theta_2} .\end{aligned}$$

And we split the left hand side into

$$\frac{d-a}{d-f} = \frac{\left(\sqrt{\nu(\nu-1)}-\sqrt{(\mu-\nu)(\lambda-\nu)}\right)^2}{\lambda\mu-\lambda\nu-\mu\nu+\nu} = \frac{\theta_4^2-\theta_5^2}{\theta_4^2+\theta_5^2}$$

and

$$\begin{aligned}\frac{f-b}{a-b} &= \frac{(\nu+\sqrt{\nu^2-\nu})(\lambda+\mu-1)-\lambda\nu+\sqrt{\lambda\mu(\lambda-1)(\mu-1)}}{(\nu-\sqrt{\nu^2-\nu})(\lambda+\mu-1)-\lambda\nu+\sqrt{\lambda\mu(\lambda-1)(\mu-1)}} \\ &= 1+2\frac{(\lambda+\mu-1)\sqrt{\nu(\nu-1)}}{(\nu-\sqrt{\nu^2-\nu})(\lambda+\mu-1)-\lambda\nu+\sqrt{\lambda\nu(\lambda-1)(\nu-1)}} \\ &= 1+2\frac{\theta_2\theta_3\theta_5^2(\theta_1^2\theta_7^2\theta_9^2+\theta_2^2\theta_6^2\theta_8^2)}{\theta_5^2(\theta_0\theta_1-\theta_2\theta_3)(\theta_1^2\theta_7^2\theta_9^2+\theta_2^2\theta_6^2\theta_8^2)-\theta_6^2\theta_7^2\theta_9^2(\theta_0\theta_1\theta_9^2-\theta_2\theta_3\theta_8^2)} ,\end{aligned}$$

which when combined together gives

$$\begin{aligned}\frac{(b-f)(a-d)}{(d-f)(a-b)} &= \left(1+2\frac{\theta_2\theta_3\theta_5^2(\theta_1^2\theta_7^2\theta_9^2+\theta_2^2\theta_6^2\theta_8^2)}{\theta_5^2(\theta_0\theta_1-\theta_2\theta_3)(\theta_1^2\theta_7^2\theta_9^2+\theta_2^2\theta_6^2\theta_8^2)-\theta_6^2\theta_7^2\theta_9^2(\theta_0\theta_1\theta_9^2-\theta_2\theta_3\theta_8^2)}\right)\left(\frac{\theta_4^2-\theta_5^2}{\theta_4^2+\theta_5^2}\right)\\ &= 1+2\frac{-\theta_5^2\left(\theta_0\theta_1\theta_2^2\theta_3^2(-\theta_4^4+\theta_5^4)-\theta_2\theta_3(\theta_1^2\theta_4^2\theta_7^2\theta_9^2+\theta_2^2\theta_4^2\theta_6^2\theta_8^2-\theta_6^2\theta_7^2\theta_8^2\theta_9^2)\right)}{(\theta_5^2(\theta_0\theta_1-\theta_2\theta_3)(\theta_1^2\theta_7^2\theta_9^2+\theta_2^2\theta_6^2\theta_8^2)-\theta_6^2\theta_7^2\theta_9^2(\theta_0\theta_1\theta_9^2-\theta_2\theta_3\theta_8^2))(\theta_4^2+\theta_5^2)}\\ &= 1+2\frac{\Theta_3}{\Theta_4}\ .\end{aligned}$$

Note that we have omitted many of the simplifications using theta relations in an attempt to be more succinct. Therefore to complete the argument it amounts to showing that

$$\Theta_1\Theta_4-\Theta_2\Theta_3=0\ .$$

This was done using symbolic manipulation with Maple. The aim is to rewrite the expression with as few θ_i's as possible and hope that the terms cancel out. The first step was to use relations such as

$$\theta_6^2\theta_7^2=\theta_0^2\theta_1^2-\theta_2^2\theta_3^2$$

to eliminate all θ_6^2, θ_7^2, θ_8^2 and θ_9^2. Note that this is always possible; that is, any two products of these four functions can be written as the combination of the remaining theta functions. This results in a homogenous polynomial of degree 16 in the six remaining theta functions with roughly 60 terms. Next using the two relations

$$\theta_4^2\theta_5^2=\theta_0^2\theta_3^2-\theta_1^2\theta_2^2\quad\text{and}\quad\left(\theta_4^4+\theta_5^4\right)=\theta_0^4-\theta_1^4-\theta_2^4+\theta_3^4$$

one can reduce the powers of θ_4 and θ_5. At this stage Maple returned a factorisation of the form

$$\theta_2\theta_3F(\theta_0,\theta_1,\theta_2,\theta_3,\theta_4,\theta_5)(\theta_0^2\theta_3^2-\theta_1^2\theta_2^2-\theta_4^2\theta_5^2)\ ,$$

where F is a degree 12 polynomial with eight terms. But we know from the theta identities that the second bracket vanishes and thus this proves (2.2).

Finally for (2.3) we have, on the right,

$$\begin{aligned}\left(\frac{\theta_0(2\Omega)\theta_1(2\Omega)}{\theta_6(2\Omega)\theta_7(2\Omega)}\right)^2 &= 1+2\frac{(\theta_0\theta_3+\theta_1\theta_2)(\theta_0\theta_2+\theta_1\theta_3)}{(\theta_0^2+\theta_1^2-\theta_2^2-\theta_3^2)(\theta_0\theta_1-\theta_2\theta_3)}\\ &= 1+2\frac{\Theta_1}{\Theta_2}\ .\end{aligned}$$

And on the left we have

$$\frac{e-a}{e-f} = \frac{\left(\sqrt{\nu(\nu-1)} + \sqrt{(\mu-\nu)(\lambda-\nu)}\right)^2}{\lambda\mu - \lambda\nu - \mu\nu + \nu} = \frac{\theta_4^2 + \theta_5^2}{\theta_4^2 - \theta_5^2}$$

which gives (we have already computed the other term previously)

$$\begin{aligned}\frac{(b-f)(a-e)}{(e-f)(a-b)} &= 1 + 2\frac{\theta_5^2\left(\theta_0\theta_1\theta_2^2\theta_3^2(-\theta_4^4+\theta_5^4) + \theta_2\theta_3(\theta_1^2\theta_4^2\theta_7^2\theta_9^2 + \theta_2^2\theta_4^2\theta_6^2\theta_8^2 + \theta_6^2\theta_7^2\theta_8^2\theta_9^2)\right)}{(\theta_5^2(\theta_0\theta_1 - \theta_2\theta_3)(\theta_1^2\theta_7^2\theta_9^2 + \theta_2^2\theta_6^2\theta_8^2) - \theta_6^2\theta_7^2\theta_9^2(\theta_0\theta_1\theta_9^2 - \theta_2\theta_3\theta_8^2))(\theta_4^2 - \theta_5^2)} \\ &= 1 + 2\frac{\Theta_3}{\Theta_4} \ .\end{aligned}$$

Then using the same procedure as above we see that

$$\Theta_1\Theta_4 - \Theta_2\Theta_3 = \theta_2\theta_3 F'(\theta_0,\theta_1,\theta_2,\theta_3,\theta_4,\theta_5)(\theta_0^2\theta_3^2 - \theta_1^2\theta_2^2 - \theta_4^2\theta_5^2) \ ,$$

which completes the proof since the last bracket vanishes as before. □

Note that there are many alternative choices to reduce a hyperelliptic curve to Rosenhain form. The choice made here

$$x' = \frac{x-a}{x-f}\cdot\frac{b-f}{b-a}$$

corresponds to the choice of ordering the roots $\{0, 1, \lambda, \mu, \nu\}$. Taking a different order of the roots changes the transformation required. Using the same method, we can also compute the other obtainable results via a wrong choice. One can view this as an analogue of Proposition 3.10 in [Jar08].

Proposition 2.28. *Let C be a hyperelliptic curve in Rosenhain form, given by the equation*

$$C : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

with λ, μ and ν distinct complex numbers and denote the period matrix of C by $\Omega \in \mathbb{H}_2$. Then all possible results Ω' of the AGM map are given by

$$\Omega' = 2\left(\begin{pmatrix} I_2 & 0 \\ C & I_2 \end{pmatrix}\Omega\right) = 2\Omega(C\Omega + I_2)^{-1} \ ,$$

where I_2 denotes the 2×2 identity matrix and C runs over the set

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&1\end{pmatrix} \ .$$

Proof. The right choice corresponds to taking $C = \mathbf{0}$ as shown in the previous theorem. We will compute one case explicitly; the rest follows similarly. Consider the choice where μ and ν are swapped, that is,

$$P = x(x-1)\ , \quad Q = (x-\lambda)(x-\nu)\ , \quad \text{and} \quad R = x-\mu\ .$$

Here we will only show that

$$\frac{(b'-f')(a'-c')}{(c'-f')(a'-b')} = \left(\frac{\theta_0(\Omega')\theta_9(\Omega')}{\theta_5(\Omega')\theta_7(\Omega')}\right)^2\ ,$$

where $\Omega' = 2\Omega(C\Omega + I_2)^{-1}$ with C inside the list. The corresponding values of $a', b', \ldots, f'$ changes as follows (essentially swapping all μ's and ν's):

$$\begin{aligned}
a' &= \mu - \sqrt{\mu^2-\mu}\ , \\
b' &= \frac{\lambda\nu - \sqrt{\lambda\nu(\lambda-1)(\nu-1)}}{\lambda+\nu-1}\ , \\
c' &= \frac{\lambda\nu + \sqrt{\lambda\nu(\lambda-1)(\nu-1)}}{\lambda+\nu-1}\ , \\
d' &= \mu - \sqrt{(\nu-\mu)(\lambda-\mu)}\ , \\
e' &= \mu + \sqrt{(\nu-\mu)(\lambda-\mu)}\ , \\
f' &= \mu + \sqrt{\mu^2-\mu}\ .
\end{aligned}$$

Considering the left hand side we have

$$\begin{aligned}
\frac{(b'-f')(a'-c')}{(c'-f')(a'-b')} &= \left(1 + \frac{2\lambda\nu(\mu-1) + 2\sqrt{\lambda\mu\nu(\lambda-1)(\mu-1)(\nu-1)}}{\lambda\nu-\lambda\mu-\mu\nu+\mu}\right)^2 \\
&= \left(1 + \frac{2[\theta_1^2\theta_9^2 - \theta_5^2\theta_6^2]\theta_0^4 + 2\sqrt{\theta_0^4[\theta_0^2\theta_1^2 - \theta_7^2\theta_8^2][\theta_1^2\theta_9^2 - \theta_5^2\theta_6^2][\theta_0^2\theta_9^2 - \theta_5^2\theta_7^2]}}{[\theta_0^2\theta_5^2 - \theta_7^2\theta_9^2]\theta_0^2\theta_6^2 + [\theta_6^2\theta_7^2 - \theta_0^2\theta_1^2]\theta_5^2\theta_7^2}\right)^2 \\
&= \left(1 + \frac{2\theta_0^4\theta_8^2 + 2\theta_0^2\theta_2^2\theta_8^2}{\theta_0^2\theta_4^2\theta_6^2 - \theta_2^2\theta_5^2\theta_7^2}\right)^2 \\
&= \left(1 + \frac{2\theta_0^4\theta_8^2 + 2\theta_0^2\theta_2^2\theta_8^2}{[\theta_0^2\theta_6^2\theta_4^2 - \theta_0^2\theta_2^2\theta_9^2] + [\theta_0^2\theta_2^2\theta_9^2 - \theta_2^2\theta_7^2\theta_5^2]}\right)^2 \\
&= \left(1 + \frac{2\theta_0^4 + 2\theta_0^2\theta_2^2}{\theta_2^4 - \theta_0^4}\right)^2 \\
&= \left(\frac{\theta_2^2 + \theta_0^2}{\theta_2^2 - \theta_0^2}\right)^2
\end{aligned}$$

where all these theta functions are evaluated at the original period matrix Ω. Now let $C = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and the right hand side becomes

$$\left(\frac{\theta_0(2\Omega(C\Omega+I_2)^{-1})\theta_9(2\Omega(C\Omega+I_2)^{-1})}{\theta_5(2\Omega(C\Omega+I_2)^{-1})\theta_7(2\Omega(C\Omega+I_2)^{-1})}\right)^2 = \left(\frac{\theta_8(\Omega(C\Omega+I_2)^{-1})^2+\theta_9(\Omega(C\Omega+I_2)^{-1})^2}{\theta_8(\Omega(C\Omega+I_2)^{-1})^2-\theta_9(\Omega(C\Omega+I_2)^{-1})^2}\right)^2$$
$$= \left(\frac{\theta_0(\Omega)^2+\theta_2(\Omega)^2}{\theta_0(\Omega)^2-\theta_2(\Omega)^2}\right)^2 .$$

where the first equality is identical to the previous theorem and the second equality follows from the transformation property in Theorem 2.6. Since the constant $\kappa(\mathbf{a},\mathbf{b},\gamma)$ is independent of Ω, one directly computes that this constant is 1 for both θ_8 and θ_9. □

Admittedly we have not computed all 24 equations explicitly except via numerical examples, but with the bank of theta relations available we are confident this should be easy. This gives an alternative notion of a right choice in that it is the choice which doubles the period of the hyperelliptic curve. We conjecture, through numerical examples, that this is in fact the same as the right choice we have previously defined. Nonetheless, in practice finding the minimum total value of the pair is definitely the easier method to do.

Chapter 3

Elliptic Curves over the p-adics

3.1 Uniformisation Theory

Over the complexes, one is able to associate elliptic curves with quotients of the form $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}$. An explicit isomorphism can be written down using the Weierstrass $\wp$-function:

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E(z) \\ z &\longmapsto \left(\wp(z,\Lambda), \frac{1}{2}\wp'(z,\Lambda)\right) \end{aligned}$$

which is referred as *complex uniformisation*. Furthermore, the discriminant and j-invariant of the corresponding elliptic curve can be computed explicitly (for example, see Chapter 3.1 in [Sil86]). However, this approach immediately fails if one considers curves over $\mathbb{Q}_p$. Let $\Lambda \subseteq \mathbb{Q}_p$ be a lattice, that is, a discrete additive subgroup, and let t be a non-zero element in Λ. Since $p^n t$ lies inside Λ for all n, it forms a sequence that converges to 0. So there cannot exist any non-trivial discrete subgroups in $\mathbb{Q}_p$.

The solution, first introduced by Tate, is to exponentiate first. Note that although we work with $\mathbb{Q}_p$ here, everything carries forward to any p-adic field. In this case there are plenty of discrete subgroups inside $\mathbb{Q}_p^*$; one important example is the set of powers of q, denoted $q^{\mathbb{Z}} \subseteq \mathbb{Q}_p^*$ for any $q \in \mathbb{Q}_p^*$ with $|q| < 1$. This gives the quotient $\mathbb{Q}_p^*/q^{\mathbb{Z}}$, which turns out to play the role of $\mathbb{C}/\Lambda$. The first observation is that as a complex function $\wp(z,\Lambda)$, with $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, is $\mathbb{Z}$-periodic in both variables, so we can find an explicit Fourier expansion of

$\wp(z,\Lambda)$ in terms of $u = e^{2\pi i z}$ and $q = e^{2\pi i \tau}$:

$$\frac{1}{(2\pi i)^2}\wp(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} + \frac{1}{12} \ ,$$

which gives an analytic isomorphism between $\mathbb{C}^*/q^{\mathbb{Z}}$ and $E(\mathbb{C})$ (see Chapter 5.1 in [Sil94] for details). This motivates the following power series

$$\begin{aligned} X(u,q) &= \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} \ , \\ Y(u,q) &= \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} \ , \end{aligned}$$

which converge for all $u \in \overline{\mathbb{Q}}_p^* \setminus q^{\mathbb{Z}}$. Furthermore, define

$$\begin{aligned} a_4(q) &= -5\sum_{n\geq 1}\frac{n^3 q^n}{1-q^n} \ , \\ a_6(q) &= -\frac{5}{12}\sum_{n\geq 1}\frac{n^3 q^n}{1-q^n} - \frac{7}{12}\sum_{n\geq 1}\frac{n^5 q^n}{1-q^n} \ , \end{aligned}$$

both of which have integral coefficients and hence lie in $\mathbb{Z}[\![q]\!]$. Define the *Tate curve* E_q by the equation

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q) \ .$$

This gives the following uniformisation theorem (Theorem 3.1, p. 423, in [Sil94]):

Theorem 3.1. *For $u, q \in \overline{\mathbb{Q}}_p$ with $|q| < 1$ and $u \notin q^{\mathbb{Z}}$, the Tate curve E_q is an elliptic curve, and the series $X(u,q)$ and $Y(u,q)$ define an isomorphism*

$$\begin{aligned} \phi : \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}} &\longrightarrow E_q(\overline{\mathbb{Q}}_p) \\ u &\longmapsto \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \ , \\ O & \text{if } u \in q^{\mathbb{Z}} \ . \end{cases} \end{aligned}$$

Furthermore, the map ϕ is compatible with the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*, that is,*

$$\phi(u^\sigma) = \phi(u)^\sigma$$

for all $u \in \overline{\mathbb{Q}}_p^*$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Note that the above p-adic uniformisation also holds true for any finite extension $K/\mathbb{Q}_p$.

The theorem says that every such quotient $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ corresponds to a Tate curve over $\overline{\mathbb{Q}}_p$. But it is immediately obvious that not every elliptic curve over $\mathbb{Q}_p$ is isomorphic over $\overline{\mathbb{Q}}_p$ to such a Tate curve (whereas one can show this is true over $\mathbb{C}$), since the j-invariant of the Tate curve is given by

$$|j(E_q)| = \left|\frac{1}{q} + 744 + 196884q + \cdots\right| > 1 \ ,$$

which is preserved by isomorphism. This gives a necessary condition for a p-adic curve to be uniformised in this way, and the last part of Tate's uniformisation theorem shows that this condition is in fact sufficient as well.

Theorem 3.2. *Let $E/\mathbb{Q}_p$ be an elliptic curve with $|j(E)| > 1$ and define the quantity $\gamma(E/\mathbb{Q}_p) := -c_4/c_6 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Then there exists a unique $q \in \mathbb{Q}_p^*$ with $|q| < 1$ such that $E \cong E_q$ over $\overline{\mathbb{Q}}_p$. Furthermore, the following are equivalent:*

(i) *E is isomorphic to E_q over $\mathbb{Q}_p$.*

(ii) *$\gamma(E/\mathbb{Q}_p) = 1$.*

(iii) *E has split multiplicative reduction.*

Proof. We sketch the proof following Theorem 5.3 in [Sil94] (p. 441). The fact that there exists a Tate curve E_q isomorphic to E over $\overline{\mathbb{Q}}_p$ is an exercise in formal power series. Set $j(q)$ to be the j-invariant of E_q and let $f(q)$ be the reciprocal of $j(q)$. One computes directly that

$$f(q) = \frac{q}{1 + 744q + 196884q^2 + \cdots} = q - 744q + 356652q^3 - \cdots \in \mathbb{Z}[\![q]\!] \ .$$

In particular, this means that there exists a inverse series $g(q) \in \mathbb{Z}[\![q]\!]$ such that $g(f(q)) = q$ which converges for any elements of $\overline{\mathbb{Q}}_p$ of absolute value less than 1. Now since $|j(E)| > 1$ we see that by setting

$$q = g\left(\frac{1}{j(E)}\right) \in \mathbb{Q}_p^* \ ,$$

we have $|q| < 1$,

$$\frac{1}{j(E_q)} = f(q) = f\left(g\left(\frac{1}{j(E)}\right)\right) = \frac{1}{j(E)}$$

and thus $E_q \cong E$ over $\overline{\mathbb{Q}}_p$. Uniqueness follows from the fact that $j(q) = j(q')$ implies $f(q) = f(q')$.

The quantity $\gamma(E/\mathbb{Q}_p)$ is independent of the choice of Weierstrass equation for $E/\mathbb{Q}_p$ and we omit the proof that two curves $E/\mathbb{Q}_p$ and $E'/\mathbb{Q}_p$ are isomorphic over $\mathbb{Q}_p$ if and only

if $j(E) = j(E')$ and $\gamma(E/\mathbb{Q}_p) = \gamma(E'/\mathbb{Q}_p)$. So to show that (i) and (ii) are equivalent it suffices to show that $\gamma(E_q/\mathbb{Q}_p) = 1$ modulo squares.

It follows from definition that the quantities c_4 and c_6 of E_q are given by

$$c_4(q) = 1 - 48a_4(q) = 1 + 240\sum_{n\geq 1}\frac{n^3q^n}{1-q^n} \ ,$$
$$c_6(q) = -1 + 72a_4(q) - 864a_6(q) = -1 + 504\sum_{n\geq 1}\frac{n^5q^n}{1-q^n} \ ,$$

where one notes that

$$\left|\sum_{n\geq 1}\frac{n^3q^n}{1-q^n}\right| = \left|\sum_{n\geq 1}\frac{n^5q^n}{1-q^n}\right| = |q| < 1 \ .$$

Now a direct computation shows that

$$(1+4\alpha)^{-\frac{1}{2}} = \sum_{n=0}^{\infty}\binom{-\frac{1}{2}}{n}(4\alpha)^n = \sum_{n=0}^{\infty}(-1)^n\binom{2n}{n}\alpha^n \in \mathbb{Z}[\![\alpha]\!] \ ,$$

so that $(1+4\alpha)$ is a square in $\mathbb{Q}_p$ for all $|\alpha| < 1$. This implies that

$$\gamma(E_q/\mathbb{Q}_p) \equiv 1 \mod \mathbb{Q}_p^{*2} \ .$$

Given that E and E_q are isomorphic over $\mathbb{Q}_p$, the reduced curve $\widetilde{E}_q$ is given by the equation $y^2 + xy = x^3$, which has a node at the point $(0,0)$ with tangent lines $y = 0$ and $y = -x$. This shows that we have split multiplicative reduction and thus (i) implies (iii).

It remains to show that (iii) implies (ii). Consider a curve $E/\mathbb{Q}_p$ with split multiplicative reduction and Weierstrass model given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ .$$

Without loss of generality, assume that the singular point of the mod p reduction is at the origin. Then the fact that $(0,0)$ lies on E and that it is singular implies that

$$a_3 \equiv a_4 \equiv a_6 \equiv 0 \mod p\mathbb{Z}_p \ .$$

This in turns means that

$$\begin{aligned} b_4 &= a_1a_3 + 2a_4 \equiv 0 \mod p\mathbb{Z}_p \ , \\ b_6 &= a_3^2 + 4a_6 \equiv 0 \mod p\mathbb{Z}_p \ , \\ c_4 &= b_2^4 - 24b_4 \equiv b_2^2 \mod p\mathbb{Z}_p \ . \end{aligned}$$

Furthermore, multiplicative reduction means that c_4 is non-zero modulo p and hence b_2 is a unit. Hence putting everything together we have

$$\gamma(E/\mathbb{Q}_p) = \frac{1}{b_2}\left(\frac{1 - 24\frac{b_4}{b_2^2}}{1 - 36\frac{b_4}{b_2^2} + 216\frac{b_6}{b_2^3}}\right) \equiv \frac{1}{b_2} \equiv b_2 \mod \mathbb{Q}_p^{*2} \ ,$$

where we argue as before that the numerator and denominators are both of the form $1+4\alpha$ and thus squares. The reduction of E modulo p has the form

$$\widetilde{E} : y^2 + \widetilde{a}_1xy = x^3 + \widetilde{a}_2x^2 \ .$$

Factoring over $\overline{\mathbb{F}}_p$ gives

$$(y - \widetilde{\alpha}x)(y - \widetilde{\beta}x) = y^2 + \widetilde{a}_1xy - \widetilde{a}_2x^2 \ ,$$

where $\widetilde{\alpha} \neq \widetilde{\beta}$ since the reduction is split. Now Hensel's lemma gives two $\alpha, \beta \in \mathbb{Q}_p$ with

$$(y - \alpha x)(y - \beta x) = y^2 + a_1xy - a_2x^2 \ .$$

This gives

$$b_2 = a_1^2 + 4a_2 = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 \in \mathbb{Q}_p^{*2}$$

and we are done. □

For an elliptic curve $E/\mathbb{Q}_p$ with Tate uniformisation $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$, we call this q the *period* of the elliptic curve. We end with the following corollary:

Corollary 3.3. *Let $E/\mathbb{Q}_p$ be an elliptic curve with $|j(E)| > 1$ and $q \in \mathbb{Q}_p^*$ such that $E \cong E_q$ over $\overline{\mathbb{Q}}_p$. Then E is isomorphic to E_q over the field $L = \mathbb{Q}_p(\sqrt{\gamma(E/\mathbb{Q}_p)})$.*

3.2 p-adic AGM

We now turn to a notion of AGM for p-adic numbers introduced by Henniart and Mestre in [HM89], as well as its application to compute p-adic periods of elliptic curves.

We start with some basic notations. Let K be a p-adic field and denote the maximal ideal of the ring of integers of K by $\mathfrak{m}_K$. If $x \equiv 1 \mod 4\mathfrak{m}_K$, then by $\sqrt{x}$ we mean the unique element y of K such that $y^2 = x$ and $y \equiv 1 \mod 2\mathfrak{m}_K$. Now let α and β be elements of $K^\times$ such that $\alpha \equiv \beta \mod 8\mathfrak{m}_K$. We define two corresponding sequences $\{\alpha_n\}$ and $\{\beta_n\}$ by first setting $\alpha_0 = \alpha$ and $b_0 = \beta$, then using the iterative algorithms

$$\alpha_{n+1} = \frac{\alpha_n + \beta_n}{2} \quad \text{and} \quad \beta_{n+1} = \beta_n \sqrt{\frac{\alpha_n}{\beta_n}} \ .$$

For odd p, this simply means that if we have $\alpha_n \equiv \beta_n \mod \mathfrak{m}_K$, then take the square root $\sqrt{\alpha_n \beta_n}$ such that $\alpha_{n+1} \equiv \beta_{n+1} \mod \mathfrak{m}_K$. As with real numbers we immediately see that since

$$|\alpha_{n+1} - \beta_{n+1}| = \frac{\left|\sqrt{\alpha_n} - \sqrt{\beta_n}\right|^2}{2} = \frac{|\alpha_n - \beta_n|^2}{2\left|\sqrt{\alpha_n} + \sqrt{\beta_n}\right|^2} \leq \frac{|\alpha_n - \beta_n|^2}{|8\beta|} \ ,$$

the sequences $\{\alpha_n\}$ and $\{\beta_n\}$ converge quadratically to the same element in K^*; we write $M(\alpha, \beta)$ for this *arithmetic-geometric mean* of α and β.

Consider an elliptic curve E/K given by the equation

$$E : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \ .$$

Suppose it has a non-integral j-invariant, and hence by the discussion in the previous section it admits a Tate uniformisation $E_q = \overline{K}^*/q^{\mathbb{Z}}$ for some $q \in \mathfrak{m}_K$. Then we saw that E and E_q are isomorphic over $K' = K(\sqrt{\gamma(E/K)})$. It is well known (for example, see p. 44 in [Sil86]) that any isomorphisms between E and E_q are given by simple change of variables of the form

$$x = u^2 x' + r \quad \text{and} \quad y = u^3 y' + s u^2 x' + v$$

for some $r, s, u, v \in \overline{K}_p$ and $u \neq 0$. Pick one of the two isomorphisms ϕ from E_q to E (the other being $-\phi$), then it induces a map between the canonical differentials of E and E_q via multiplication by u. That is, explicitly we have

$$\phi^* \left(\frac{dx}{2y} \right) = u \frac{dt}{t} \ ,$$

where t is the parameter of the Tate curve. Since u is given by the square root of some power seires here, we see that u^2, which is independent of the choice of ϕ, lives inside K. We now describe an algorithm to compute u^2 based on the p-adic arithmetic-geometric mean following [HM89], where we fill in some of the omitted details in the paper.

Let

$$\begin{aligned} P_1 &= \phi(-1) = (e_1, 0) \ , \\ P_2 &= \phi(-\sqrt{q}) = (e_2, 0) \ , \\ P_3 &= \phi(\sqrt{q}) = (e_3, 0) \end{aligned}$$

be the three non-trivial points of order 2 on E. In particular, P_1 is characterised by the fact that $\left|12e_1^2 + 2b_2e_1 + 2b_4\right|_\pi = \left|\frac{c_4}{16}\right|_\pi$; furthermore, $\sqrt{12e_1^2 + 2b_2e_1 + 2b_4} \in K$ since we have seen in the proof of Theorem 3.2 that $c_4 \equiv b_2^2 \mod \mathfrak{m}_K$. By split multiplicative reduction we also have $e_2 \equiv e_3 \mod \mathfrak{m}_K$, and e_1 reduces to a simple root modulo $\mathfrak{m}_K$.

Let L denote the field extension $K'(\sqrt{q})$ and $\mathbf{m}_L$ the maximal ideal of the ring of integers $\mathcal{O}_L$. We then have $(e_2 - e_1) \equiv (e_3 - e_1) \mod 16\mathbf{m}_L$ and therefore one can choose square roots of $\sqrt{e_3 - e_1}$ and $\sqrt{e_2 - e_1}$ satisfying the congruence relation $\sqrt{e_3 - e_1} \equiv \sqrt{e_2 - e_1} \mod 8\mathbf{m}_L$. Denote their arithmetic-geometric mean $M(\sqrt{e_2 - e_1}, \sqrt{e_3 - e_1}) \in L$.

Theorem 3.4. *Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ by an elliptic curve over $\mathbb{Q}_p$ with non-integral j-invariant. Denote E_q the Tate curve associated with E and let ϕ be an isomorphism between E and E_q such that*

$$\phi^* \left(\frac{dx}{2y} \right) = u \frac{dt}{t} \ .$$

Then we have

$$u = \frac{1}{2M(\sqrt{e_2 - e_1}, \sqrt{e_3 - e_1})} \ .$$

Proof. First denote the formal power series by

$$\theta(z) = \sum_{n\in\mathbb{Z}} z^{n^2}$$

(of course, as a formal series this is just the standard theta function). Define an elliptic curve over $\mathbb{Q}_p$ by the equation

$$E' : y^2 = x\left(x - \theta^4\left(\sqrt{q}\right)\right)\left(x - \theta^4\left(-\sqrt{q}\right)\right) \ .$$

By directly computing the j-invariant from its coefficients, one sees that this indeed has the same j-invariant as E_q (i.e. given by the series $q^{-1} + 744 + 196884q + \cdots$). Hence there exists a unique isomorphism $\psi : E_q \longrightarrow E'$ such that the induced map satisfies

$$\psi^*\left(\frac{dx}{2y}\right) = \frac{dt}{t} \ .$$

Furthermore, since the points of order two on E_q are given by the points $(-1, 0)$, $(-\sqrt{q}, 0)$ and $(\sqrt{q}, 0)$, by denoting the x-coordinate of $\psi(-1)$, $\psi(-\sqrt{q})$ and $\psi(\sqrt{q})$ by ε_1, ε_2 and ε_3 respectively we immediately see that

$$\varepsilon_1 = 0, \quad \varepsilon_2 = \theta^4\left(-\sqrt{q}\right) \quad \text{and} \quad \varepsilon_3 = \theta^4\left(\sqrt{q}\right) \ .$$

By composing the maps $\phi \circ \psi^{-1} : E' \longrightarrow E$, we see that

$$\begin{aligned} 2u\sqrt{e_2 - e_1} &= \sqrt{\varepsilon_2 - \varepsilon_1} = \theta^2\left(-\sqrt{q}\right) \ , \\ 2u\sqrt{e_3 - e_1} &= \sqrt{\varepsilon_3 - \varepsilon_1} = \theta^2\left(\sqrt{q}\right) \ . \end{aligned}$$

Note that as formal power series, $\theta^2\left(\sqrt{q}\right)$ and $\theta^2\left(-\sqrt{q}\right)$ are simply $\theta_{0,0}\left(\frac{1}{\pi i}\ln(\sqrt{q})\right)$ and $\theta_{0,1}\left(\frac{1}{\pi i}\ln(\sqrt{q})\right)$ respectively and thus we know that

$$M\left(\theta^2\left(\sqrt{q}\right), \theta^2\left(-\sqrt{q}\right)\right) = 1$$

Combining with the basic properties of the arithmetic-geometric mean gives

$$2uM(\sqrt{e_2 - e_1}, \sqrt{e_3 - e_1}) = 1$$

and we are done. □

Note that since $M(\alpha, \beta)$ lies in L, the above theorem requires calculations inside L whereas in fact u^2 is an element of K. With a slight modification all calculations can be shifted down into K. We first define a modified arithmetic-geometric mean for α and β in K^* with $\alpha \equiv \beta \mod 16\mathfrak{m}_K$ by setting $\alpha_0 = \alpha$ and $b_0 = \beta$. But for $n \geq 1$ we use the formulae

$$\beta_{n+1} = \sqrt{\alpha_n \beta_n} \quad \text{and} \quad \alpha_{n+1} = \frac{\alpha_n + \beta_n + 2\beta_{n+1}}{4}$$

instead. Let $M'(\alpha, \beta)$ denote the common limit of the sequences $\{\alpha_n\}$ and $\{\beta_n\}$. We note this is merely the square of the arithmetic-geometric mean of $\sqrt{\alpha}$ and $\sqrt{\beta}$:

Lemma 3.5. *Let $\alpha, \beta \in K^*$ such that $\alpha \equiv \beta \mod 16\mathfrak{m}_K$. Then we have*

$$M'(\alpha, \beta) = M\left(\sqrt{\alpha}, \sqrt{\beta}\right)^2 .$$

Proof. It suffices to show that the i-th term of the left hand side is the square of the i-th term of the right hand side for all i. But this is clear since

$$\alpha_{n+1} = \frac{\alpha_n + \beta_n + 2\beta_{n+1}}{4} = \left(\frac{\sqrt{\alpha_n} + \sqrt{\beta_n}}{2}\right)^2 .$$

Hence in the limit $M'(\alpha, \beta) = M\left(\sqrt{\alpha}, \sqrt{\beta}\right)^2$ as required. □

It follows immediately that the calculations required to compute $M'(\alpha, \beta)$ are all done over K instead of L. The following proposition allows one to compute u^2 from this modified AGM process.

Proposition 3.6. *Let*

$$\alpha = \frac{4\sqrt{12e_1^2 + 2b_2e_1 + 2b_4} - 12e_1 - b_2}{16} \quad \textit{and} \quad \beta = \frac{\sqrt{12e_1^2 + 2b_2e_1 + 2b_4}}{2} ,$$

where the square root is taken such that $4\sqrt{12e_1^2 + 2b_2e_1 + 2b_4} \equiv -12e_1 - b_2 \mod 2\mathfrak{m}_K$. Then we have

$$u^2 = \frac{1}{4M'(\alpha, \beta)} .$$

In particular, all calculations are done over K.

Proof. In view of the previous lemma, the proposition amounts to showing that

$$M(\sqrt{\alpha}, \sqrt{\beta}) = M(\sqrt{e_2 - e_1}, \sqrt{e_3 - e_1}) \ ,$$

where recall that we have

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x - e_1)(x - e_2)(x - e_3) \ .$$

We show that $\sqrt{\alpha}$ and $\sqrt{\beta}$ are in fact the arithmetic and geometric mean of $\sqrt{e_2 - e_1}$ and $\sqrt{e_3 - e_1}$ respectively. That is to say, $(\sqrt{\alpha}, \sqrt{\beta})$ is simply the first iteration of the arithmetic-geometric mean, from which the proposition follows.

This follows from direct computations. Factorising the right hand side of the curve gives

$$x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x - e_1)\left[x^2 + \left(e_1 + \frac{b_2}{4}\right)x + \left(e_1^2 + \frac{e_1 b_2}{4} + \frac{b_4}{2}\right)\right]$$

and therefore we must have

$$e_2, e_3 = \frac{1}{2}\left(-e_1 - \frac{b_2}{4} \pm \sqrt{\left(e_1 + \frac{b_2}{4}\right)^2 - 4\left(e_1^2 + \frac{e_1 b_2}{4} + \frac{b_4}{2}\right)}\right) \ ,$$

whence

$$\sqrt{e_2 - e_1}, \sqrt{e_3 - e_1} = \left[\frac{1}{2}\left(-3e_1 - \frac{b_2}{4} \pm \sqrt{\left(e_1 + \frac{b_2}{4}\right)^2 - 4\left(e_1^2 + \frac{e_1 b_2}{4} + \frac{b_4}{2}\right)}\right)\right]^{\frac{1}{2}} \ .$$

Finally we see that

$$\begin{aligned}
\sqrt{(e_2 - e_1)(e_3 - e_1)} &= \frac{1}{2}\left[\left(-3e_1 - \frac{b_2}{4}\right)^2 - \left(e_1 + \frac{b_2}{4}\right)^2 - 4\left(e_1 + \frac{e_1 b_2}{4} + \frac{b_4}{2}\right)\right]^{\frac{1}{2}} \\
&= \frac{1}{2}\left(4e_1^2 + 2b_2 e_1 + 2b_4\right)^{\frac{1}{2}} \\
&= \beta
\end{aligned}$$

and

$$\begin{aligned}\left(\frac{\sqrt{e_2-e_1}+\sqrt{e_3-e_1}}{2}\right)^2 &= \frac{1}{4}\left(e_2+e_3-2e_1+2\sqrt{(e_2-e_1)(e_3-e_1)}\right)\\ &= \frac{1}{4}\left(-e_1-\frac{b_2}{4}-2e_1+\sqrt{4e_1+2b_2e_1+2b_4}\right)\\ &= \frac{1}{4}\left(-3e_1-\frac{b_2}{4}+\sqrt{4e_1^2+2b_2e_1+2b_4}\right)\\ &= \alpha\ ,\end{aligned}$$

which proves the proposition. Note that $\sqrt{12e_1^2+2b_2e_1+2b_4}$ lies in K and hence the last claim follows immediately. □

To compute the period q of the elliptic curve, we also need a p-adic analogue of the classical Landen transformation which was introduced in the first chapter. The p-adic analogue of the algorithm is a quadratically convergent algorithm which computes the preimage $\phi^{-1}(P) \in \overline{K}^*/q^{\mathbb{Z}}$ given any $P \in E(\overline{K})$.

The key idea is to construct a tower of 2-isogenies using the AGM process. Begin by considering an elliptic curve $E = E_0$ over K with non-integral j-invariant given by the equation

$$E_0 : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x-e_1)(x-e_2)(x-e_3)\ .$$

As above, define quantities

$$\begin{aligned}\alpha = \alpha_0 &= \frac{4\sqrt{12e_1^2+2b_2e_1+2b_4}-12e_1-b_2}{16}\ ,\\ \beta = \beta_0 &= \frac{\sqrt{12e_1^2+2b_2e_1+2b_4}}{2}\end{aligned}$$

with $4\sqrt{12e_1^2+2b_2e_1+2b_4} \equiv -12e_1-b_2 \mod 2\mathfrak{m}_K$. Using the associated AGM sequences $\{\alpha_n\}$ and $\{\beta_n\}$, construct a sequence of elliptic curves $\{E_n\}$ for $n \geq 1$ by the equation

$$E_n : y^2 = x(x+\alpha_n)(x+\alpha_n-\beta_n)\ .$$

The j-invariant of these curves are all non-integral and thus each of these E_n admits a Tate uniformisation, which will be denoted $E_{q^{2^n}}$. There are also isomorphisms $\phi_n : E_{q^{2^n}} \longrightarrow E_n$ associated to each Tate curve, and $\phi_0 = \phi$ is the isomorphism we wish to understand. In fact, these ϕ_n are computed explicitly in Chapter 5.1 of [Sil94] (note that the maps given

there are from $\overline{K}^*/q^{\mathbb{Z}} \to E_q$ so we composed it with multiplication by u):

$$\phi_n(t) = \left(\frac{1}{u^2} \sum_{n\in\mathbb{Z}} \frac{q^n t}{1-q^n t} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2},\ \frac{1}{2u^3} \sum_{n\in\mathbb{Z}} \frac{q^n t(1+q^n t)}{(1-q^n t)^3} \right) .$$

There exist 2-isogenies from $g_i : E_{i+1} \longrightarrow E_i$ for $i \geq 0$ given by the formulae

$$g_i(x',y') = \begin{cases} \left(x + \dfrac{\alpha_0(\alpha_0-\beta_0)}{x} - \dfrac{4e_1+b_2}{8},\ y\left(1 - \dfrac{\alpha_0(\alpha_0-\beta_0)}{x^2}\right)\right) & \text{for } i = 0 , \\ \left(x + \dfrac{\alpha_i(\alpha_i-\beta_i)}{x} - \dfrac{\alpha_{i-1}-\beta_{i-1}}{2},\ y\left(1 - \dfrac{\alpha_i(\alpha_i-\beta_i)}{x^2}\right)\right) & \text{for } i \geq 1 . \end{cases}$$

We check that this is (assuming $i \geq 1$ for simplicity) indeed a well-defined isogeny by direct computation. Since the modified AGM gives

$$\frac{\alpha_i+\beta_i}{2} = 2\alpha_{i+1} - \beta_{i+1} \quad \text{and} \quad \left(\frac{\alpha_{i-1}-\beta_{i-1}}{4}\right)^2 = \alpha_i(\alpha_i-\beta_i) ,$$

we have

$$\begin{aligned} & x'(x'+\alpha_i)(x'+\alpha_i-\beta_i) \\ &= \frac{1}{x^3}\left(\left[x^2+\alpha_i(\alpha_i-\beta_i)\right]^2 - \left[\frac{\alpha_{i-1}-\beta_{i-1}}{2}\right]^2 x^2 \right) \left(x^2+\alpha_i(\alpha_i-\beta_i)+(2\alpha_i-\beta_i)x\right) \\ &= \frac{1}{x^3}\left(\left[x^2+\alpha_i(\alpha_i-\beta_i)\right]^2 - 4\alpha_i(\alpha_i-\beta_i)x^2 \right) (x+\alpha_i)\left(x+\alpha_i-\beta_i\right) \\ &= \frac{1}{x^4}\left(x^2-\alpha_i(\alpha_i-\beta_i)\right)^2 \left[x\left(x+\alpha_i\right)\left(x+\alpha_i-\beta_i\right)\right] \\ &= y^2\left(1-\frac{\alpha_i(\alpha_i-\beta_i)}{x^2}\right)^2 \end{aligned}$$

which proves the claim.

The kernel of the isogeny is generated by the point of order 2 $(0,0) \in E_{i+1}(\overline{K})$. By directly differentiating we see that

$$\frac{d}{dx}\left(x + \frac{\alpha_i(\alpha_i-\beta_i)}{x} - \frac{\alpha_{i-1}-\beta_{i-1}}{2}\right) = 1 - \frac{\alpha_i(\alpha_i-\beta_i)}{x^2} = \frac{y'}{y}$$

and hence

$$g_i^*\left(\frac{dx}{2y}\right) = \frac{dx'}{2y'}$$

for all i. This means that when one considers the sequence of isomorphisms ϕ_n, the maps

on differentials are given by

$$\phi_i^*\left(\frac{dx}{2y}\right) = u\frac{dt}{t}$$

for all i. That is, u is in fact independent of i. Now as n tends to infinity, the equation of E_n tends to

$$E_\infty : y^2 = x^2(x + M'(\alpha, \beta)) \ .$$

Furthermore, since $|q| < 1$, q^n tends to 0 and the only term left in $\phi_\infty : \overline{K}^* \longrightarrow E_\infty$ is the term with $n = 0$. This gives

$$\phi_\infty(t) = \left(\frac{t}{u^2(1-u)}, \ \frac{t(1+t)}{2u^3(1-t)^3}\right) \ .$$

The situation can be summarised in the following commutative diagram

$$\begin{array}{ccccccccccc}
\overline{K}^* & \cdots & \longrightarrow & \overline{K}^*/q^{2^{n+1}\mathbb{Z}} & \xrightarrow{f_n} & \overline{K}^*/q^{2^n\mathbb{Z}} & \longrightarrow & \cdots & \longrightarrow & \overline{K}^*/q^{2\mathbb{Z}} & \xrightarrow{f_0} & \overline{K}^*/q^{\mathbb{Z}} \\
\downarrow{\scriptstyle \phi_\infty} & & & \downarrow{\scriptstyle \phi_{n+1}} & & \downarrow{\scriptstyle \phi_n} & & & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_0 = \phi} \\
E_\infty & \cdots & \longrightarrow & E_{n+1} & \xrightarrow{g_n} & E_n & \longrightarrow & \cdots & \longrightarrow & E_1 & \xrightarrow{g_0} & E_0 = E
\end{array}$$

Note that the maps f_i are simply the identity maps since ϕ_i^* is multiplication by u (for all i) and g_i^* is the identity map on differentials. Let $P_0(x_0, y_0) \in E(\overline{K})$ and let $t_\infty \in \overline{K}^*$ be the unique preimage $\phi^{-1}(P_0)$ such that $0 \leq |t_\infty| < |q|$. Then for all $n \geq 0$, by working modulo q^{2^n} one puts $t_n = t_\infty \mod q^{2^n}$ and obtains $P_n(x_n, y_n) = \phi_n(t_n) \in E_n(\overline{K})$. The key idea is that by using the explicit formulae for g_i, one can work backwards on the bottom row of the diagram and compute the point $P_\infty(x_\infty, y_\infty) \in E_\infty(\overline{K})$, which is the limit of the $P_i(x_i, y_i)$. Now computing $\phi_\infty^{-1}(P_\infty)$ is easy due to the simple form which ϕ_∞ takes.

Now actually inverting the isogenies g_i is a relatively simple matter of algebraic manipulations. For $i = 0$, solving the quadratic for x and y gives

$$\begin{aligned}
x &= \frac{1}{16}\left(8x' + 4e_1 + b_2 + \sqrt{(8x' + 4e_1 + b_2)^2 - 256\,\alpha_0(\alpha_0 - \beta_0)}\right) \\
&= \frac{1}{2}\left(x_0 + \frac{4e_1 + b_2}{8}\right)\left(1 + \sqrt{1 - \frac{256\,\alpha_0(\alpha_0 - \beta_0)}{(8x_0 + 4e_1 + b_2)^2}}\right) \ , \\
y &= y'\left(1 - \frac{\alpha_0(\alpha_0 - \beta_0)}{x^2}\right)^{-1} \\
&= y'\left(\frac{x^2}{x^2 - \alpha_0(\alpha_0 - \beta_0)}\right) \ .
\end{aligned}$$

And for $i \geq 1$

$$\begin{aligned}
x &= \frac{1}{4}\left(2x' + \alpha_{i-1} - \beta_{i-1} + \sqrt{(2x' + \alpha_{i-1} - \beta_{i-1})^2 - 16\,\alpha_i(\alpha_i - \beta_i)}\right) \\
&= \frac{x'}{4}\left(2 + \frac{\alpha_{i-1} - \beta_{i-1}}{x'} + \sqrt{\left(2 + \frac{\alpha_{i-1} - \beta_{i-1}}{x'}\right)^2 - \frac{(\alpha_{i-1} - \beta_{i-1})^2}{x'^2}}\right) \\
&= \frac{x'}{4}\left(2 + \frac{\alpha_{i-1} - \beta_{i-1}}{x'} + 2\sqrt{1 + \frac{\alpha_{i-1} - \beta_{i-1}}{x'}}\right) \\
&= \frac{x'}{4}\left(1 + \sqrt{1 + \frac{\alpha_{i-1} - \beta_{i-1}}{x'}}\right)^2 , \\
y &= y'\left(\frac{x^2}{x^2 - \alpha_i(\alpha_i - \beta_i)}\right) \\
&= y'\left(\frac{16x^2}{16x^2 - (\alpha_{i-1} - \beta_{i-1})^2}\right) .
\end{aligned}$$

At the limit we have

$$(x_\infty, y_\infty) = \left(\frac{t_\infty}{u^2(1-u)},\ \frac{t_\infty(1+t_\infty)}{2u^3(1-t_\infty)^3}\right)$$

and solving for the first coordinate gives

$$t_\infty + \frac{1}{t_\infty} = 2 + \frac{1}{u^2 x_\infty} .$$

Furthermore we have

$$2uy_\infty = \frac{t_\infty(1+t_\infty)}{u^2(1-t_\infty)^2(1-t_\infty)} = x_\infty\left(\frac{1+t_\infty}{1-t_\infty}\right)$$

which gives t_∞ as a function of u, x_∞ and y_∞ by

$$t_\infty = \frac{2uy_\infty - x_\infty}{2uy_\infty + x_\infty} .$$

The following algorithm summarises the above.

Algorithm 3.7 (p-adic Landen's transformation)**.**
Input: An elliptic curve E/K with split multiplicative reduction given by

$$E : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

with roots e_1, e_2 and e_3 such that $e_2 \equiv e_3 \mod \mathfrak{m}_K$; $P_0 = (x_0, y_0)$ a point on $E(K)$.
Ouput: The preimage $\phi^{-1}(P) \in \overline{K}^*/q^{\mathbb{Z}}$ in the Tate uniformisation.

1. *Let $\alpha_0 = \alpha$ and $\beta_0 = \beta$. Compute $P_1(x_1, y_1)$ from the equations*

$$x_1 = \frac{1}{2}\left(x_0 + \frac{4e_1 + b_2}{8}\right)\left(1 + \sqrt{1 - \frac{256\alpha_0(\alpha_0 - \beta_0)}{(8x_0 + 4e_1 + b_2)^2}}\right) ,$$
$$y_1 = y_0\left(\frac{x_1^2}{x_1^2 - \alpha_1(\alpha_1 - \beta_1)}\right) .$$

2. *For $n \geq 1$, compute $P_{n+1}(x_{n+1}, y_{n+1})$, α_{n+1} and β_{n+1} from the formulae*

$$x_{n+1} = \frac{x_n}{4}\left(1 + \sqrt{1 + \frac{\alpha_{n-1} - \beta_{n-1}}{x_n}}\right)^2 ,$$
$$y_{n+1} = y_n\left(\frac{16x_{n+1}^2}{16x_{n+1}^2 - (\alpha_{n-1} - \beta_{n-1})^2}\right) ,$$
$$\beta_{n+1} = \sqrt{\alpha_n\beta_n} ,$$
$$\alpha_{n+1} = \frac{\alpha_n + \beta_n + 2\beta_{n+1}}{4} .$$

3. *Let $P_\infty(x_\infty, y_\infty)$ be the limit of P_n. We then have*

$$u^2 = \frac{1}{4M'(\alpha, \beta)} ,$$
$$t_\infty = \frac{2uy_\infty - x_\infty}{2uy_\infty + x_\infty} ,$$
$$t_\infty + \frac{1}{t_\infty} = 2 + \frac{1}{u^2 x_\infty} ,$$

where $t_\infty = \phi^{-1}(P_0)$ is the preimage of the isomorphism $\phi : E_q \longrightarrow E$.

Note that if P_0 and u are rational over K, then all calculations are done over K. This allows one to compute the period q by applying the above algorithm to the point at infinity $\mathcal{O} = (0 : 1 : 0)$. The first step of the algorithm simply gives the two 2-torsion points on E_1. At this point we take the non-trivial point $(0, 0)$ and proceed as in Algorithm 3.7. By the

choice of $\mathcal{O}$ we know that $\phi^{-1}(\mathcal{O}) = q$ whence

$$q + \frac{1}{q} = 2 + \frac{1}{u^2 x_\infty} \ ,$$

which gives

$$q = 1 + \frac{1}{2u^2 x_\infty} - \sqrt{\frac{4u^2 x_\infty + 1}{4u^4 x_\infty^2}} \ .$$

This gives a quadratically convergent algorithm to compute q compared to linear procedures such as inverting the power series of the j-invariant. See [HM89] for a worked example.

3.3 Coleman Integration

We end this chapter on a slight digression on a perhaps surprising link between the AGM and p-adic integration. Since p-adic spaces are totally disconnected by nature, finding a p-adic analogue of antidifferentiation turned out to be a challenge. Coleman introduced a notion of integration based on the principle of *Frobenius equivariance*, and we will outline the basics of the theory here. This requires some rigid analytic geometry which will be omitted; see [BGR84] for example for an introduction to the topic.

Let $\mathbb{C}_p$ be a completed algebraic closure of $\mathbb{Q}_p$ and denote $\mathcal{O}$ its valuation subring. Also let Log denote a branch of the p-adic logarithm, that is, a homomorphism from $\mathbb{C}_p^\times \to \mathbb{C}_p$ such that its restriction to the disc $\{x \in \mathbb{C}_p : |x-1| < 1\}$ is given by the usual logarithm series $\sum_{i=1}^{\infty}(1-x)^i/i$. For an open interval $I \subseteq [0, +\infty)$, write $A(I)$ for the disc $\{t \in \mathbb{A}^1_{\mathbb{C}_p} : |t| \in I\}$. We first define integrals on these discs by the formula

$$\int_P^Q \sum_{i\in\mathbb{Z}} c_i t^i dt := c_{-1}\mathrm{Log}\left(\frac{Q}{P}\right) + \sum_{i\neq -1} \frac{c_i}{i+1}(Q^{i+1} - P^{i+1}) \ .$$

where P and Q are points in $A(I)$ and $\sum_i c_i t^i dt$ is a differential in $\Omega^1_{A(I)/\mathbb{C}_p}$. Note that this does not allow one to integrate on closed discs because of the $i+1$ in the denominator.

A *curve* over the valuation ring $\mathcal{O}$ is a smooth proper connected scheme X over $\mathcal{O}$ of relative dimension 1. Consider the function field $K(X)$ equipped with the p-adic absolute value, then the elements of $K(X)$ of norm at most 1 give the local ring in X of the generic point of the special fibre $\overline{X}$ of X. Let $X_{\mathbb{Q}}$ denote the generic fibre of X as a rigid analytic space, then there is a natural specialisation map from $X_{\mathbb{Q}}$ to $\overline{X}$.

A *residue disc* of X is an open unit disc which is isomorphic to the inverse image of a point of $\overline{X}$. Given a curve X, a *wide open subspace* of $X_{\mathbb{Q}}$ is a rigid analytic subspace of $X_{\mathbb{Q}}$ of the form $\{x \in X_{\mathbb{Q}} : |f(x)| < \lambda\}$ for some $f \in K(X)$ of absolute value 1 and some $\lambda > 1$.

Under these settings, Coleman found a notion of p-adic integration that exhibits no path dependence, which we quote from [Bal15].

Theorem 3.8. *For each curve X over $\mathcal{O}$ and each wide open subspace W of $X_{\mathbb{Q}}$, there exists a map*

$$\mu_W : \mathrm{Div}^0(W) \times \Omega^1_{W/\mathbb{C}_p} \longrightarrow \mathbb{C}_p$$

with the following properties:

(i) *Linearity: The map μ_W is linear on $\mathrm{Div}^0(W)$ and $\mathbb{C}_p$-linear on $\Omega^1_{W/\mathbb{C}_p}$.*

(ii) *Compatibility: For any residue disc D of X and any isomorphism $\varphi : W \cap D \to A(I)$ for some interval I, the restriction of μ_W to $\mathrm{Div}^0(W \cap D) \times \Omega^1_{W/\mathbb{C}_p}$ agrees with the notion of integration on $A(I)$ via φ.*

(iii) *Change of variables: Let X' be another curve over $\mathcal{O}$ and W' be a wide open subspace of X'. Let $\varphi : W \to W'$ be any morphism of rigid spaces relative to an automorphism of $\mathbb{C}_p$. Then*

$$\mu_{W'}(\varphi(\cdot), \cdot) = \mu_W(\cdot, \varphi^*(\cdot)) \ .$$

(iv) *Fundamental theorem of calculus: For any $Q = \sum_i c_i(P_i) \in \mathrm{Div}^0(W)$ and $f \in \mathcal{O}(W)$,*

$$\mu_W(Q, df) = \sum_i c_i f(P_i) \ .$$

We will not delve into the theory as much since our focus here is more on the computational side of the spectrum – Coleman's theory is principally very suitable for numerical computation, and Balakrishnan developed this idea in the case of hyperelliptic curves. We cover some of the ideas following [BBK10] and [Bal15]. Let X be a hyperelliptic curve of genus g with model of the form $y^2 = f(x)$, where $f(x)$ has degree $2g + 1$.

For P and Q in the same residue disc (Weierstrass or not), the corresponding integral from P to Q is called a *tiny integral*. Integrals of this form are performed by first computing a parameterisation of the path between P and Q, then integrating the resulting power series formally. The parameterisation used depends on the disc which the points P and Q lie in:

Algorithm 3.9 (Parameterisation of path between two points)**.**
Input: Two points $P, Q \in X(\mathbb{C}_p)$ in the same residue disc.
Ouput: Parameterisation $(x(t), y(t))$ of the path between P and Q.

- *If P and Q lie in a non-Weierstrass residue disc, then a parameterisation is given by*

  1. *Let $x(t) = t + a$, where $P = (a, b)$ and t is a local coordinate.*
  2. *Obtain $y(t) = \sqrt{f(x(t))}$ by Newton's method; that is, let $y_0(t) = b$ and*

  $$y_i(t) = \frac{1}{2}\left(y_{i-1} + \frac{f(x(t))}{y_{i-1}(t)}\right)$$

  for $i \geq 1$.

- *If P and Q lie in a finite Weierstrass residue disc, then a parameterisation is given by*

  1. *Let $y(t) = t + b$, where $P = (a, b)$ and t is a local coordinate.*
  2. *Obtain $x(t)$ by Newton's method; that is, let $x_0(t) = a$ and*

  $$x_i(t) = x_{i-1}(t) - \frac{f(x_{i-1}(t)) - y(t)^2}{f'(x_{i-1}(t))}$$

  for $i \geq 1$.

- *If P and Q are both points at infinity, then a parameterisation is given by*

  1. *Take $x_0 = t^{-2}$ and let $h(x, t) = \left(\frac{x^g}{t}\right)^2 - f(x)$ and use Newton's method to obtain*

  $$x_i(t) = x_{i-1}(t) - \frac{h(x_{i-1}(t), t)}{h'(x_{i-1}(t), t)} \ ,$$

  where $h'(x_{i-1}(t), t)$ is the partial derivative with respect to x.

  2. *Then $y(t)$ is given by*

  $$y(t) = \frac{(x(t))^g}{t} \ .$$

The following algorithm computes integrals of the basis differentials $\omega_i = \dfrac{x^i dx}{2y}$ using the parameterisation just described.

Algorithm 3.10 (Computing tiny integrals)**.**
Input: Two points $P, Q \in X(\mathbb{C}_p)$ in the same residue disc and a basis differential ω_i.
Ouput: Tiny Coleman integral between P and Q.

1. *Construct a parameterisation of the path from P to Q using Algorithm 3.9.*

2. *Substitute it into the integral and formally integrate the power series in t:*

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^{t(Q)} \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt \ .$$

For computing Coleman integrals from P to Q on different residue discs one uses the Frobenius to move between residue discs, or formally perform an *analytic continuation along Frobenius*. The rough idea is to first find *Teichmüller points* P' and Q' which lie in the same residue discs as P and Q respectively. These are points which are fixed by the Frobenius Φ, that is, $\Phi(P') = P'$ and $\Phi(Q') = Q'$. The Frobenius can then be used to compute the integral from P' to Q', and by additivity we obtain

$$\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i + \int_{Q'}^{Q} \omega_i \ .$$

But our aim here is to compute tiny integrals using a p-adic AGM and thus we will not go into the details of general Coleman integrations. Interested readers should consult one of the aforementioned papers.

Now let $E/\mathbb{Q}_p$ be an elliptic curve given by $y^2 = (x-e_1)(x-e_2)(x-e_3)$ such that the roots satisfy $(e_2 - e_1) \equiv (e_3 - e_1) \mod p\mathbb{Z}_p$. Suppose now that P and Q are points on $E(\mathbb{Q}_p)$ inside the same residue disc. Then recall from Theorem 3.1 that ϕ is an isomorphism from $E_q \longrightarrow E$ such that the induced map satisfies

$$\phi^* \left(\frac{dx}{2y} \right) = u \frac{dt}{t} \ .$$

Therefore combining it with fundamental properties of the Coleman integral in Theorem 3.8 one sees that

$$\int_P^Q \frac{dx}{2y} = \int_{\phi^{-1}(P)}^{\phi^{-1}(Q)} \phi^* \left(\frac{dx}{2y} \right) = \int_{\phi^{-1}(P)}^{\phi^{-1}(Q)} u \frac{dt}{t} = u \ \mathrm{Log} \left(\frac{\phi^{-1}(Q)}{\phi^{-1}(P)} \right) \ .$$

This gives the following:

Algorithm 3.11 (Computing tiny integrals for split multiplicative curves)**.**
Input: An elliptic curve with split multiplicative reduction $E/\mathbb{Q}_p$ with Weierstrass points $(e_i, 0)$ and $P, Q \in E(\mathbb{Q}_p)$ in the same residue disc.
Ouput: Tiny Coleman integral between P and Q.

1. *Let $\alpha = e_2 - e_1$ and $\beta = e_3 - e_1$, where $e_2 \equiv e_3 \mod p$.*
2. *Compute the quantity $u^2 \in \mathbb{Q}_p$ using Proposition 3.6.*
3. *Applying the Landen's transformation to both P and Q, compute the preimage $\phi^{-1}(P)$ and $\phi^{-1}(Q)$.*
4. *We then have*
$$\int_P^Q \frac{dx}{2y} = u \operatorname{Log}\left(\frac{\phi^{-1}(Q)}{\phi^{-1}(P)}\right) .$$

For example, consider the elliptic curve E over $\mathbb{Q}_7$ given by

$$E : y^2 = (x-1)(x-2)(x-9) .$$

Now consider the two points P and Q given by

$$\begin{aligned} P &= (5, 1 + 3 \times 7^2 + 3 \times 7^3 + 2 \times 7^4 + 4 \times 7^5 + \cdots) , \\ Q &= (5 + 7, 1 + 6 \times 7 + 2 \times 7^2 + 3 \times 7^3 + 2 \times 7^4 + 3 \times 7^5 + \cdots) . \end{aligned}$$

Then the above procedure gives

$$\begin{aligned} u &= 3 + 4 \times 7 + 7^2 + 6 \times 7^3 + 2 \times 7^4 + 6 \times 7^5 , \\ \phi^{-1}(P) &= 5 + 5 \times 7^2 + 4 \times 7^3 + 2 \times 7^4 + 3 \times 7^5 , \\ \phi^{-1}(Q) &= 5 + 2 \times 7 + 7^2 + 2 \times 7^3 + 6 \times 7^4 + 7^5 \end{aligned}$$

and hence

$$\int_P^Q \frac{dx}{2y} = 4 \times 7 + 5 \times 7^2 + 5 \times 7^3 + 2 \times 7^4 + 5 \times 7^5 + \cdots .$$

This agrees with the inbuilt function of Sage (which uses Algorithm 3.10 and integrates term by term); one can turn to Appendix B to find Sage codes of the above algorithm.

Chapter 4

Genus 2 Curves over the p-adics

4.1 Introduction

We begin with a quick review of the situation in genus 1 over p-adic fields, where every elliptic curve $E = E_0$ with split multiplicative reduction over a p-adic field K can be uniformised with a Tate curve $E_q = \overline{K}^*/q^{\mathbb{Z}}$. The AGM process creates an isogenous elliptic curve E_1 with period q^2; hence by iterating the AGM one obtains a chain of elliptic curves and their respective Tate curves:

$$\begin{array}{ccccccccccc}
\overline{K}^* & \cdots & \longrightarrow & \overline{K}^*/q^{2^{n+1}\mathbb{Z}} & \xrightarrow{f_n} & \overline{K}^*/q^{2^n\mathbb{Z}} & \longrightarrow & \cdots & \longrightarrow & \overline{K}^*/q^{2\mathbb{Z}} & \xrightarrow{f_0} & \overline{K}^*/q^{\mathbb{Z}} \\
\downarrow{\scriptstyle \phi_\infty} & & & \downarrow{\scriptstyle \phi_{n+1}} & & \downarrow{\scriptstyle \phi_n} & & & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_0=\phi} \\
E_\infty & \cdots & \longrightarrow & E_{n+1} & \xrightarrow{g_n} & E_n & \longrightarrow & \cdots & \longrightarrow & E_1 & \xrightarrow{g_0} & E_0 = E
\end{array}$$

We have also seen how to compute the period using the AGM: the key in the algorithm relies on inverting the vertical maps ϕ_i's. Although each ϕ_i is given by some complicated power series which makes it hard to work with, in the limit these maps degenerate into a simple expression which can be inverted.

Moving on to genus 2, the other ingredient comes from the Bost-Mestre AGM for genus 2 which is a realisation of the Richelot isogeny between hyperelliptic curves. As shown in [Smi05], it is a $(2,2)$-correspondence, and therefore composing it with its dual gives the doubling map on the Jacobian of the original curve. The equations defining this correspondence are also easy to write down, as we have seen in Chapter 2, which makes it easy to manipulate in theory. The vital observation is that this map doubles the periods of a hyperelliptic curve, suggesting that it is the right map to consider.

The situation over p-adic fields is less well understood. The Tate curves are replaced by what we now call *Mumford curves*, after Mumford showed in 1972 that if a genus g curve has 'bad enough' (but not too bad) reduction over a p-adic field, then there exists an analytic parameterisation which generalises Tate's work (in fact his work was far beyond that, extending to abelian varieties over local rings, though we will not touch upon that here). The maps g_i's in the above diagram are replaced by the Richelot isogenies. Since the equations are simple algebraic expressions, it is clear that they are well-defined over any p-adic fields as well.

The vertical maps ϕ_i's, however, remain somewhat mysterious. In [Kad07], Kadziela gives a description via the theory of automorphic forms; but these are infinite products which are hard to work with practically. On the other hand Teitelbaum, in [Tei88], describes these maps using p-adic theta functions and even inverts them to compute the periods; however his method is linear, akin to computing the period of a Tate curve by inverting the power series of its j-invariant.

Our aim is therefore to combine the aforementioned theories to develop a quadratically convergent algorithm to compute periods of p-adic hyperelliptic curves using the Richelot isogeny. We begin by covering the necessary background to understand the basics of Mumford curves, including the theory of Schottky groups, automorphic forms and Jacobians of hyperelliptic curves. A discussion of the p-adic AGM and Richelot isogeny follows, as we show that they have the same doubling property as in $\mathbb{C}$. This allows one to have a full understanding on the algebraic side of the picture, especially to devise a method to lift the Richelot isogeny along the chain of isogenous hyperelliptic curves. We will demonstrate this in practice, using the modular curve $X_0(23)$ as an example.

At the time of writing, we do not yet have a concrete description of the vertical maps, which we will need in order to complete the algorithm. However, in the final section we will give reasons and insights as to why this should be feasible with a bit more time. This will hopefully be completely and published in a joint paper with Frazer Jarvis.

4.2 p-adic Analysis

Let K be a p-adic field with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ has a unique maximal ideal with uniformiser π. Let X be a curve over K; then one may study its reduction mod π. We say that X is *semi-stable* if its reduction only has singularities which are ordinary double points, and every non-singular rational component meet the other components in at least 2 points. If, in addition, all the components in its reduction are of genus zero and both tangent lines at every double point are rational, then X is called *totally split*.

Now consider a totally split hyperelliptic curve X of genus 2 over K. In this case being totally split simply means that the equation of X modulo π reduces to

$$X : y^2 \equiv (x-\alpha)^2(x-\beta)^2(x-\gamma)(x-\delta) \mod \pi \ ,$$

where α, β and γ are distinct. In [Tei88], these curves are classified into three types:

1. Type A refers to the case where δ is different from α, β and γ;
2. Type B refers to the case where $\delta \equiv \gamma \mod \pi$;
3. Type C refers to the case where $\delta \equiv \alpha \mod \pi$.

Teitelbaum mainly works with Type B curves in his work, partially because his interest were modular curves, which are of this type. Similarly we will only be concerned with curves with Type B reduction here, since it gives us a canonical way to split the sextic (although most of the general p-adic theory we describe here applies to any hyperelliptic curves, and even to higher genera).

4.2.1 Uniformisation Theory

Mumford proved in [Mum72] that every totally split curve admits a p-adic uniformisation, now called a *Mumford curve*. We give a survey of this theory mainly following [GvdP80], [Tei88] and [Kad07].

Consider the group $\mathrm{PGL}_2(K)$ for any field K which is complete with respect to some non-archimedean valuation; it is the automorphism group of $\mathbb{P}^1_K$. Then for any

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(K) \ ,$$

define the action on the projective line $\mathbb{P}^1_K$ via $\gamma(z) = \dfrac{az+b}{cz+d}$ for all $z \in \mathbb{P}^1_K$, with the usual convention for ∞ such that

$$\frac{az+b}{cz+d} = \begin{cases} \dfrac{az+b}{cz+d} & \text{if } cz+d \neq 0 \text{ and } z \neq \infty \ , \\ \infty & \text{if } cz+d = 0 \text{ and } z \neq \infty \ , \\ \dfrac{a}{c} & \text{if } z = \infty \text{ and } c \neq 0 \ , \\ 0 & \text{if } z = \infty \text{ and } c = 0 \ . \end{cases}$$

Now suppose $\Gamma \subseteq \mathrm{PGL}_2(K)$ is a subgroup. Then a point $z \in \mathbb{P}^1_K$ is called a *limit point* of Γ if there exists an infinite sequence $\{\gamma_i\}$ of distinct matrices $\gamma_i \in \Gamma$ and a point $z' \in \mathbb{P}^1_K$ such that

$$\lim_{n\to\infty} \gamma_n(z') = z \ .$$

For any given Γ, denote $\mathcal{L}(\Gamma)$ the set of all limit points of Γ. If Γ satisfies the conditions

(i) $\mathcal{L}(\Gamma) \neq \mathbb{P}^1_K$,

(ii) the orbit $\Gamma(z)$ for any point $z \in \mathbb{P}^1_K$ has a compact closure,

then we say that Γ is *discontinuous*. If K is a locally compact field, which in particular all p-adic fields are, then the second condition is automatically satisfied.

We are interested in subgroups generated by a certain type of matrix in $\mathrm{PGL}_2(K)$. We say that $\gamma \in \mathrm{PGL}_2(K)$ is *hyperbolic* if its two eigenvalues λ and μ have different valuations, that is, $|\lambda| \neq |\mu|$. The following is taken from Section 1.1 of [GvdP80].

Lemma 4.1. *A matrix $\gamma \in \mathrm{PGL}_2(K)$ is hyperbolic if and only if it is conjugate to an element of the form $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$ for some $0 < |q| < 1$.*

A subgroup $\Gamma \subseteq \mathrm{PGL}_2(K)$ is called a *Schottky group* if

(i) Γ is finitely generated;

(ii) Γ is discontinuous;

(iii) every non-trivial $\gamma \in \Gamma$ is hyperbolic.

These groups, as we will see, play the role of the subgroups $q^{\mathbb{Z}}$ in the Tate curve. We state, without proof, the structure theorem for discontinuous groups by Ihara.

Theorem 4.2.

(i) *Let Γ be a finitely generated discontinuous group. Then there exists a normal subgroup $\Gamma_0 \subseteq \Gamma$ of finite index such that Γ_0 is a Schottky group.*

(i) *Any Schottky group Γ_0 is a free group, and non-abelian if it has more than one generator.*

This is Theorem 1.3.1 from [GvdP80], where it is proved by studying the Bruhat-Tits tree of $\mathrm{PGL}_2(K)$. We also need a way to construct a space Ω along with a Schottky group on which it acts discontinuously (playing the previous role of $\overline{K}^*$). If Γ is a Schottky group, it turns out that it is sufficient to remove the limit points of Γ from $\mathbb{P}^1_K$, so that $\Omega = \mathbb{P}^1_{\mathbb{C}_p} \setminus \mathcal{L}(\Gamma)$. This also forms a fundamental domain for Γ.

Theorem 4.3. *Let Γ be a Schottky group and $\Omega = \mathbb{P}^1_{\mathbb{C}_p} \setminus \mathcal{L}(\Gamma)$. Then Γ acts discontinuously on Ω.*

In fact Ω can also be realised geometrically by cutting out open discs from the projective line. We will not go into any further details here but one thing to note is that this construction shows that Ω can be written as a union of connected domains Ω_n such that $\Omega_n \subseteq \Omega_{n+1}$ for all n and $\Omega = \bigcup_{n=1}^{\infty} \Omega_n$, where each Ω_n are obtained by cutting out finitely many open discs from the projective line.

The quotients Ω/Γ are called *Mumford curves*, due to this final theorem (Theorem 4.20 from [Mum72]) which completes the generalisation of Tate's work on elliptic curves.

Theorem 4.4. *Let Γ be a Schottky group with g generators and $\Omega = \mathbb{P}^1_{\mathbb{C}_p} \setminus \mathcal{L}(\Gamma)$. Then Ω/Γ is a smooth irreducible algebraic curve of genus g. Moreover, given an algebraic curve X over K of genus g with totally split reduction, then there exists a Schottky group with g generators such that $X \cong \Omega/\Gamma$.*

One can quickly check that this is indeed a generalisation: If $g = 1$, then Lemma 4.1 says that any hyperbolic γ is simply conjugate to some $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}_2(K)$ such that $|q| < 1$. The Schottky group Γ is then the powers of q, or equivalently $q^{\mathbb{Z}}$, with 0 and ∞ being its only limit points. Hence $\Omega = \mathbb{P}^1_{\overline{K}} \setminus \{0, \infty\} = \overline{K}^*$ and one obtains the Tate curve $\overline{K}^*/q^{\mathbb{Z}}$.

4.2.2 Automorphic Forms

Before turning our attention to automorphic forms on the space Ω, we briefly introduce some related concepts. An *affinoid disc* is a closed disc in $\mathbb{C}_p$ of the form $\mathbb{C}_p \setminus B$ for some open disc $B \subseteq \mathbb{C}_p$, and an *affinoid domain* is one that is a finite intersection of affinoid discs. For example, the fundamental domain Ω for a Schottky group can be written as a union of Ω_n, where each Ω_n is an affinoid domain by construction. The nested property of the Ω_n's makes Ω a *Stein domain* of $\mathbb{P}^1_K$.

A K-valued function on an affinoid domain is *holomorphic* (or analytic) if it is the uniform limit of rational functions with no poles in the domain. Then a function on Ω is *holomorphic* if its restriction on each Ω_n is holomorphic; the function is *meromorphic* if the restriction is the quotient of two holomorphic functions on Ω_n for all n.

Let Γ be a Schottky group. An *automorphic form* with respect to Γ is a meromorphic function f on $\Omega = \mathbb{P}^1_{\mathbb{C}_p} \setminus \mathcal{L}(\Gamma)$ satisfying the transformation property

$$f(z) = \phi(\gamma) f(\gamma(z))$$

for all $\gamma \in \Gamma$, and $\phi(\gamma) \in \mathbb{C}_p^\times$ is called the *automorphy factor*.

The results from this section come from Section 2 of [GvdP80].

Theorem 4.5. *Let $a, b \in \Omega$. Then the function*

$$\theta(a, b; z) := \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}$$

is an automorphic form on Ω with constant factors of automorphy.

These are called *p-adic theta functions* (not to be confused with the Riemann theta functions) and are, as we will see, the building blocks of all automorphic forms on Ω. But before doing so we briefly write down some of the basic properties that $\theta(a, b; z)$ satisfies.

Proposition 4.6. *We have the following:*

(i) *If $\Gamma a \neq \Gamma b$, then $\theta(a, b; z)$ has simple zeroes at Γa, simple poles at Γb and no zeros or poles elsewhere.*

(ii) *For all $\gamma \in \Gamma$, $\theta(a, b; z)$ satisfies $\theta(a, b; z) = \theta(\gamma(a), \gamma(b); z)$.*

We also wish to understand the automorphy factor of $\theta(a, b; z)$, which as it turns out is closely related to a special case of the theta function.

Proposition 4.7. *We have the following:*

(i) *The function $\theta(z_0, \gamma(z_0); z)$ is an analytic function with no zeroes on Ω. Furthermore, it is independent of the point z_0. That is, for all $z_0, z_0' \in \Omega$ and $\gamma \in \Gamma$, we have*

$$\theta(z_0, \gamma(z_0); z) = \theta(z_0', \gamma(z_0'); z) \ .$$

(ii) *For all $\gamma_1, \gamma_2 \in \Gamma$ we have*

$$\theta(z_0, \gamma_1(z_0); z)\theta(z_0, \gamma_2(z_0); z) = \theta(z_0, \gamma_1\gamma_2(z_0); z) \ .$$

(iii) *The automorphy factor $c(a, b; \gamma)$ of $\theta(a, b; z)$ depends on both a and b. In particular,*

$$c(a, b; \gamma) = \frac{\theta(z_0, \gamma(z_0); a)}{\theta(z_0, \gamma(z_0); b)}$$

and is a group homomorphism from $\Gamma \to K^*$ satisfying $c(a, b; \gamma_1\gamma_2) = c(a, b; \gamma_1)c(a, b; \gamma_2)$.

The final result on the theory of automorphic forms is the structure theorem that every automorphic form on Ω is a finite product of some theta functions.

Theorem 4.8. *Let Γ be a Schottky group and f be an automorphic form with respect to Γ on Ω. Then*

$$f(z) = c_f \prod_{i=1}^{k} \theta(a_i, b_i; z)$$

for some $a_i, b_i \in \Omega$ and $c_f \in \mathbb{C}_p^\times$ a constant. Furthermore, the automorphy factor is given by the product of the individual factors

$$c_f = \prod_{i=1}^{k} c(a_i, b_i; \gamma) \ .$$

4.2.3 The Jacobian and Periods of p-adic Schottky Groups

For every totally split p-adic curve X, we now have an algebraic curve Ω/Γ. To link these Mumford curves to the Jacobian (and thus periods) of X, we describe the work of [MD73].

Let $X_\Gamma = \mathrm{Hom}(\Gamma, K^\times)$ be the set of homomorphisms from Γ to $K^\times$. Then X_Γ is an algebraic torus. Now define a pairing $\langle \cdot, \cdot \rangle : \Gamma \times \Gamma \longrightarrow K^\times$ by

$$\langle \alpha, \beta \rangle = \frac{\theta(z_0, \alpha(z_0); z)}{\theta(z_0, \alpha(z_0); \beta(z))} \ ,$$

where z_0 is any point in Ω (recall that the function $\theta(z_0, \gamma(z_0); z)$ is independent of z_0).

Lemma 4.9. *The pairing $\langle \cdot, \cdot \rangle$ is bilinear, symmetric and its* ord *is positive definite.*

For a proof see Theorem 1 of [MD73]. The above pairing gives us a way to embed the group Γ into the torus X_Γ by sending an element $\gamma \in \Gamma$ to the function

$$\chi_\gamma(\alpha) = \langle \gamma, \alpha \rangle = \frac{\theta(z_0, \gamma(z_0); z)}{\theta(z_0, \gamma(z_0); \alpha(z))} \ .$$

One might notice that the definition of χ_γ resembles that of the automorphy factor of a p-adic theta function. In fact, for each homomorphism $\chi \in \mathrm{Hom}(\Gamma, K^\times)$, there exists a unique automorphic form f_χ on Ω whose automorphy factor is precisely χ (cf. Proposition 6.3.4 in [GvdP80]). This defines a map from $X_\Gamma/\Gamma \longrightarrow J(X)$ by mapping χ to $[\mathrm{Div}(f_\chi)]$, the class of the divisor of f_χ. This is the corresponding uniformisation of the Jacobian.

We now specialise to $g = 2$. Let γ_1 and γ_2 be the generators of our Schottky group Γ. Consider the abelianisation $\overline{\Gamma} = \Gamma/[\Gamma, \Gamma]$, then as above we obtain a pairing $\overline{\Gamma} \times \overline{\Gamma} \longrightarrow K^\times$. Take $\alpha, \beta \in \overline{\Gamma}$, where one may write $\alpha \equiv \gamma_1^{m_1}\gamma_2^{m_2}$ and $\beta \equiv \gamma_1^{n_1}\gamma_2^{n_2}$. Since the pairing is bilinear and symmetric, we have

$$\langle \alpha, \beta \rangle = \langle \gamma_1, \gamma_1 \rangle^{m_1 n_1} \langle \gamma_1, \gamma_2 \rangle^{m_1 n_2 + m_2 n_1} \langle \gamma_2, \gamma_2 \rangle^{m_2 n_2} \ .$$

In particular, the pairing is completely determined by the effects on the two generators. In [Tei88], a third element γ_3 is defined such that $\gamma_1\gamma_2\gamma_3 = 1$, and the (fundamental) *p-adic periods* are defined by

$$q_1 = \langle \gamma_2, \gamma_3 \rangle^{-1}, \quad q_2 = \langle \gamma_1, \gamma_3 \rangle^{-1} \quad \text{and} \quad q_3 = \langle \gamma_1, \gamma_2 \rangle^{-1} \ .$$

It is clear that these three periods determine the pairing.

For a genus 2 Mumford curve of Type B, the Weierstrass points are canonically partitioned according to their reductions into three pairs, S_1, S_2 and S_3. We label these the points within each pair arbitrarily as $S_i = \{(P_i^+, 0), (P_i^-, 0)\}$. Now define *half-periods* via

$$p_1 = \chi_{P_1^+,P_2^+}(\gamma_2), \quad p_2 = \chi_{P_2^+,P_3^+}(\gamma_3) \quad \text{and} \quad p_3 = \chi_{P_3^+,P_1^+}(\gamma_1) \ ,$$

where

$$\chi_{a,b}(\alpha) = \frac{\theta(z_0, \alpha(z_0); a)}{\theta(z_0, \alpha(z_0); b)}$$

is the automorphy factor of $\theta(a, b; z)$ (that is, a homomorphism $\Gamma \longrightarrow K^\times$, not to be confused with the homomorphism $\chi_\gamma : \Gamma \longrightarrow X_\Gamma$). The name is justified by the fact that $p_i^2 = q_i^{-1}$ (see Lemma 18 of [Tei88]).

Once generators are fixed for Γ, there is a natural isomorphism $\mathrm{Hom}(\Gamma, K^\times) \xrightarrow{\sim} (K^\times)^2$ given by mapping χ to the point $(\chi(\gamma_1), \chi(\gamma_2)) \in (K^\times)^2$. The image of Γ under this isomorphism is generated by the two points

$$(\chi_{\gamma_1}(\gamma_1), \chi_{\gamma_1}(\gamma_2)) = (\langle\gamma_1, \gamma_1\rangle, \langle\gamma_1, \gamma_2\rangle) = (q_2 q_3, q_3^{-1})$$

and

$$(\chi_{\gamma_2}(\gamma_1), \chi_{\gamma_2}(\gamma_2)) = (\langle\gamma_2, \gamma_1\rangle, \langle\gamma_2, \gamma_2\rangle) = (q_3^{-1}, q_1 q_3) \ .$$

Thus the image of Γ is the subgroup

$$H_\Gamma = \left\{ \left(q_2^a q_3^{a-b}, q_1^b q_3^{b-a} \right) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

which gives an isomorphism

$$X_\Gamma/\Gamma \xrightarrow{\sim} (K^\times)^2/H_\Gamma \ .$$

4.3 The Genus 2 p-adic AGM

Let X be a totally split hyperelliptic curve of genus 2 over a p-adic field K. To define a p-adic analogue of the Bost-Mestre's arithmetic-geometric mean, we require the curve to have Type B reduction. By Hensel's Lemma the curve factors into three quadratics over $\mathbb{Q}_p$, although the roots themselves may lie in a quadratic extension. Therefore, we will assume

that X is given by an equation of the form

$$X : y^2 = (x-\alpha)^2(x-\beta)^2(x-\gamma)^2 \mod \pi \ .$$

This is a *quadratic splitting* of X and is canonical for this type of curves (up to reordering α, β and γ); it plays the role of the natural ordering of roots over $\mathbb{R}$. Now define three quadratics P, Q and R using this quadratic splitting of X such that

$$P \equiv (x-\alpha)^2 \mod \pi, \quad Q \equiv (x-\beta)^2 \mod \pi \quad \text{and} \quad R \equiv (x-\gamma)^2 \mod \pi$$

and compute U, V and W as before. In this case one sees that

$$\begin{aligned} U = Q'R - R'Q &\equiv c_1(x-\beta)(x-\gamma) \mod \pi \ , \\ V = R'P - P'R &\equiv c_2(x-\alpha)(x-\gamma) \mod \pi \ , \\ W = P'Q - Q'P &\equiv c_3(x-\alpha)(x-\beta) \mod \pi \ . \end{aligned}$$

This process, similar to the situation over the real or complex numbers, takes X to a Richelot-isogenous curve $\widetilde{X}$.

By reordering the roots appropriately and defining P', Q' and R' such that $P' \equiv P \mod \pi$, $Q' \equiv Q \mod \pi$ and $R' \equiv R \mod \pi$, one can iterate this process to obtain a chain of hyperelliptic curves. We claim that the six p-adic numbers converge quadratically in pairs to three numbers.

Lemma 4.10. *The AGM process over K is quadratically convergent.*

Proof. We assume that $p > 2$ here (if $p = 2$ then we require the roots to lie in a disc of smaller radius). Say the equation of X is given by the quadratic splitting $y^2 = PQR$, where the two roots of P, Q and R are congruent to α, β and γ respectively modulo π.

If a_1 and a_2 denote the roots of P, write $a = \dfrac{a_1 + a_2}{2}$. Then we can write $a_1 = a - \varepsilon_a$ and $a_2 = a + \varepsilon_a$, and similarly for Q and R:

$$\begin{aligned} P &= (x-a_1)(x-a_2) = x^2 - 2ax + (a^2 - \varepsilon_a^2) \ , \\ Q &= (x-b_1)(x-b_2) = x^2 - 2bx + (b^2 - \varepsilon_b^2) \ , \\ R &= (x-c_1)(x-c_2) = x^2 - 2cx + (c^2 - \varepsilon_c^2) \end{aligned}$$

Let $v = \min\{v(\varepsilon_a), v(\varepsilon_b), v(\varepsilon_c)\} \geq 1$, where v denotes the valuation on K. It suffices to show that the roots of U, V and W agree up to valuation $2v$. We simply compute $U = Q'R - R'Q$ as

$$U = (b-c)x^2 + (c^2 - b^2 + \varepsilon_b^2 - \varepsilon_c^2)x + (bc(b-c) + b\varepsilon_c^2 - c\varepsilon_b^2) \ ,$$

where a factor of 2 has been taken out (since it is a unit). Solving it gives

$$\begin{aligned} u_1, u_2 &= \frac{b^2 - c^2 + \varepsilon_c^2 - \varepsilon_b^2 \pm \sqrt{(b^4 + c^4 - 2b^2c^2 + O(2v)) - 4(b-c)(bc(b-c) + O(2v))}}{2(b-c)} \\ &= \frac{b^2 - c^2 + O(2v) \pm \sqrt{(b-c)^4 + O(2v)}}{2(b-c)} \\ &= \frac{b^2 - c^2 + O(2v) \pm (b-c)^2 + O(2v)}{2(b-c)} \ , \end{aligned}$$

where $O(2v)$ denotes terms with valuation of at least $2v$ such as ε_b^2 and ε_c^2. Since $2(b-c)$ is a unit, this further simplifies to

$$u_1 = \frac{b^2 - c^2 + (b-c)^2 + O(2v)}{2(b-c)} = \frac{2b^2 - 2bc + O(2v)}{2(b-c)} = b + O(2v)$$

and

$$u_2 = \frac{b^2 - c^2 - (b-c)^2 + O(2v)}{2(b-c)} = \frac{2bc - 2c^2 + O(2v)}{2(b-c)} = c + O(2v) \ .$$

This proves that the roots of UVW agree pairwise to precision double that of PQR. □

This gives the following important corollary:

Corollary 4.11. *If X is a totally split curve with Type B reduction, then so is the Richelot isogenous curve $\widetilde{X}$. In particular, both of them admit p-adic uniformisations.*

If we write the equation of X as

$$y^2 = (x-a)(x-a')(x-b)(x-b')(x-c)(x-c') \ ,$$

where the quadratic splitting is made obvious by the notation, by taking the appropriate linear transformation of the form

$$x' = \frac{x-a}{x-c} \cdot \frac{b-c}{b-a} \ ,$$

one can transform the equation of X into Rosenhain form

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

such that a, b and c are mapped to 0, 1 and ∞ respectively. As before, there are many alternative choices to reduce the same curve. From the equation of X, we see that in the reduction modulo π, the transformation moves a', b' and c' to 0, 1 and ∞ respectively as well. That is, we have $|\lambda|_\pi > 1$, $|\mu|_\pi < 1$ and $|\nu - 1|_\pi < 1$; by abuse of notation we say $\lambda \equiv \infty \mod \pi$ from now on.

4.3.1 Riemann Theta Functions

We now show this analogue of the arithmetic-geometric mean is equivalent to doubling the half periods. To do this we consider the theta function in [Tei88], a homomorphism in X_Γ defined by

$$\theta(\chi) = \sum_{\gamma \in \overline{\Gamma}} (\gamma, \gamma)\chi(\gamma) \ ,$$

where recall that $\overline{\Gamma} = \Gamma/[\Gamma, \Gamma]$. Here the pairing $(\cdot, \cdot)$ is defined on the three generators γ_1, γ_2 and γ_3 of Γ such that

$$p_1 = (\gamma_2, \gamma_3)^{-1}, \quad p_2 = (\gamma_1, \gamma_3)^{-1} \quad \text{and} \quad p_3 = (\gamma_1, \gamma_2)^{-1} \ .$$

This is related to the bilinear and symmetric pairing $\langle \cdot, \cdot \rangle$ by the fact that $(\cdot, \cdot)^2 = \langle \cdot, \cdot \rangle$.

Now take an element $\gamma = \gamma_1^i \gamma_2^j \in \overline{\Gamma}$ and compute that

$$\begin{aligned}
\theta(\chi) &= \sum_{i,j \in \mathbb{Z}} (\gamma_1^i \gamma_2^j, \gamma_1^i \gamma_2^j)\chi(\gamma_1^i \gamma_2^j) \\
&= \sum_{i,j \in \mathbb{Z}} (\gamma_1, \gamma_1)^{i^2} (\gamma_1, \gamma_2)^{2ij} (\gamma_2 \gamma_2)^{j^2} \chi(\gamma_1)^i \chi(\gamma_2)^j \\
&= \sum_{i,j \in \mathbb{Z}} (p_2 p_3)^{i^2} p_3^{-2ij} (p_1 p_3)^{j^2} \chi(\gamma_1)^i \chi(\gamma_2)^j \\
&= \sum_{i,j \in \mathbb{Z}} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \chi(\gamma_1)^i \chi(\gamma_2)^j \ .
\end{aligned}$$

Recall that given any two points $a, b \in K$, one can define a homomorphism $\chi_{a,b}(\alpha)$ as the automorphy factor of some automorphic form. This means that for the six Weierstrass points P_1^+, P_1^-, P_2^+, P_2^-, P_3^+, P_3^-, choosing any two of them gives a homomorphism and hence a theta function. Hence this gives 16 theta functions in genus 2: there are 15 ways to pick two points, along with the trivial character. Their action on the generators γ_i are recorded in Table 1 of [Tei88] whence one can work out their series expansions easily.

For example consider the homomorphism $\chi_{P_1^+,P_2^-}$, where the table gives

$$\chi_{P_1^+,P_2^-}(\gamma_1) = p_2^{-1} \quad \text{and} \quad \chi_{P_1^+,P_2^-}(\gamma_2) = p_1^{-1} \ .$$

Then we can compute

$$\begin{aligned}
\theta(\chi_{P_1^+,P_2^-}) &= \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \chi_{P_1^+,P_2^-}(\gamma_1)^i \chi_{P_1^+,P_2^-}(\gamma_2)^j \\
&= \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} (p_2)^{-i} (p_1)^{-j} \\
&= \sum_{i,j\in\mathbb{Z}} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2} \ .
\end{aligned}$$

As expected there are six odd theta functions, which occurs when the two points have the same signs, for example P_1^+ and P_2^+. The following are the series expansions for all ten even theta functions (the above calculation gives θ_5):

$$\begin{aligned}
\theta_0 &= \theta(\chi_{\mathrm{id}}) = \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \ , \\
\theta_1 &= \theta(\chi_{P_1^+,P_1^-}) = \sum_{i,j\in\mathbb{Z}} (-1)^j p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \ , \\
\theta_2 &= \theta(\chi_{P_2^+,P_2^-}) = \sum_{i,j\in\mathbb{Z}} (-1)^i p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \ , \\
\theta_3 &= \theta(\chi_{P_3^+,P_3^-}) = \sum_{i,j\in\mathbb{Z}} (-1)^{i+j} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \ , \\
\theta_4 &= \theta(\chi_{P_1^-,P_2^+}) = \sum_{i,j\in\mathbb{Z}} (-1)^{i+j} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2} \ , \\
\theta_5 &= \theta(\chi_{P_1^+,P_2^-}) = \sum_{i,j\in\mathbb{Z}} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2} \ , \\
\theta_6 &= \theta(\chi_{P_2^-,P_3^+}) = \sum_{i,j\in\mathbb{Z}} (-1)^j p_1^{j^2} p_2^{i^2+i} p_3^{(i-j)^2+(i-j)} \ , \\
\theta_7 &= \theta(\chi_{P_2^+,P_3^-}) = \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2+i} p_3^{(i-j)^2+(i-j)} \ , \\
\theta_8 &= \theta(\chi_{P_3^-,P_1^+}) = \sum_{i,j\in\mathbb{Z}} (-1)^i p_1^{j^2+j} p_2^{i^2} p_3^{(i-j)^2-(i-j)} \ , \\
\theta_9 &= \theta(\chi_{P_3^+,P_1^-}) = \sum_{i,j\in\mathbb{Z}} p_1^{j^2+j} p_2^{i^2} p_3^{(i-j)^2-(i-j)} \ .
\end{aligned}$$

Note that our labelling simply follows the order they are printed in [GM17], but we have also included θ_0, which corresponds to the trivial character. It is easy to see that these functions converge nicely:

Lemma 4.12. *The θ_i's converge uniformly on domains of the form*

$$U^{a,b} = \{(p_1, p_2, p_3) \in \mathbb{C}_p^3 : |p_1| < |\pi_K|^a, \, |p_2| < |\pi_K|^b, \, |p_3| \leq 1\} \ ,$$

where a and b are positive rational numbers.

Proof. On the domains $U^{a,b}$ we have

$$\mathrm{ord}_K \left(p_1^{i^2} p_2^{j^2} p_3^{(i-j)^2} \right) \geq i^2 a + j^2 b$$

which tends to infinity as i and j tend to infinity. □

The following is the important link between these theta functions and the complex theta functions:

Proposition 4.13. *Let* $\Omega = \dfrac{1}{\pi i} \begin{pmatrix} \log(p_2 p_3) & -\log(p_3) \\ -\log(p_3) & \log(p_1 p_3) \end{pmatrix}$. *Then as formal power series in p_1, p_2 and p_3, we have the following identities:*

$$\begin{aligned}
\theta_0 &= \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1\ n_2)\Omega(n_1\ n_2)^{\mathrm{T}}} \ , \\
\theta_1 &= \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1\ n_2)\Omega(n_1\ n_2)^{\mathrm{T}} + \pi i n_2} \ , \\
\theta_2 &= \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1\ n_2)\Omega(n_1\ n_2)^{\mathrm{T}} + \pi i n_1} \ , \\
\theta_3 &= \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1\ n_2)\Omega(n_1\ n_2)^{\mathrm{T}} + \pi i (n_1+n_2)} \ , \\
\theta_4 &= (p_1 p_2)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1+\frac{1}{2}\ n_2+\frac{1}{2})\Omega(n_1+\frac{1}{2}\ n_2+\frac{1}{2})^{\mathrm{T}} + \pi i (n_1+n_2+1)} \ , \\
\theta_5 &= (p_1 p_2)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1+\frac{1}{2}\ n_2+\frac{1}{2})\Omega(n_1+\frac{1}{2}\ n_2+\frac{1}{2})^{\mathrm{T}}} \ , \\
\theta_6 &= (p_2 p_3)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1+\frac{1}{2}\ n_2)\Omega(n_1+\frac{1}{2}\ n_2)^{\mathrm{T}} + \pi i n_2} \ , \\
\theta_7 &= (p_2 p_3)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i (n_1+\frac{1}{2}\ n_2)\Omega(n_1+\frac{1}{2}\ n_2)^{\mathrm{T}}} \ ,
\end{aligned}$$

$$\theta_8 = (p_1p_3)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i(n_1\ n_2+\frac{1}{2})\Omega(n_1\ n_2+\frac{1}{2})^{\mathrm{T}}+\pi i n_1} ,$$
$$\theta_9 = (p_1p_3)^{-\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i(n_1\ n_2+\frac{1}{2})\Omega(n_1\ n_2+\frac{1}{2})^{\mathrm{T}}} .$$

Proof. This is done by direct computation; we only do θ_4 as an example. Expanding the term inside the exponent gives

$$\log(p_2p_3)^{\left(n_1+\frac{1}{2}\right)^2} - 2\log(p_3)^{\left(n_1+\frac{1}{2}\right)\left(n_2+\frac{1}{2}\right)} + \log(p_1p_3)^{\left(n_2+\frac{1}{2}\right)^2} .$$

Thus the power of p_1 (after exponentiating) is

$$\left(n_2+\frac{1}{2}\right)^2 = (n_2^2+n_2)+\frac{1}{4} .$$

Similarly for p_2 and p_3 we have

$$\left(n_1+\frac{1}{2}\right)^2 = (n_1^2+n_1)+\frac{1}{4}$$

and

$$\left(n_1+\frac{1}{2}\right)^2 - 2\left(n_1+\frac{1}{2}\right)\left(n_2+\frac{1}{2}\right) + \left(n_2+\frac{1}{2}\right)^2 = (n_1-n_2)^2$$

respectively. Therefore, after relabelling the summation wtih $n_1 = i-1$ and $n_2 = j-1$ one finds that

$$\sum_{(n_1,n_2)\in\mathbb{Z}^2} e^{\pi i(n_1+\frac{1}{2}\ \ n_2+\frac{1}{2})\Omega(n_1+\frac{1}{2}\ \ n_2+\frac{1}{2})^{\mathrm{T}}+\pi i(n_1+n_2+1)} = (p_1p_2)^{\frac{1}{4}}\theta_4$$

and the proposition follows. □

This means that these functions are, at least as power series, basically the same as the ones over $\mathbb{C}$. The upshot of this is that all the duplication formulae from Chapter 2 hold here as well (with minor adjustments to account for the terms outside the summation). We also note in passing that the numbering of theta functions in Section 2.5 was chosen so that they would align with the p-adic theta functions.

4.4 Period Doubling

Now consider the model of X of the form

$$X : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

such that

$$\lambda \equiv \infty \mod \pi\ , \quad \mu \equiv 0 \mod \pi \quad \text{and} \quad \nu \equiv 1 \mod \pi\ .$$

Given a general sextic model, this is always possible by translating one root to 0, one to 1 and a third to infinity (recall that X is totally split of Type B). Our work is based on the following Theorem 28 in [Tei88]:

Theorem 4.14. *The roots of X in the above form can be expressed by the theta functions such that*

$$\lambda = \left(1 - \left(\frac{\theta_3\theta_6}{\theta_2\theta_7}\right)^2\right)^{-1}, \quad \mu = 1 - \left(\frac{\theta_3\theta_9}{\theta_1\theta_8}\right)^2 \quad \textit{and} \quad \nu = \left(\frac{\theta_2\theta_4}{\theta_1\theta_5}\right)^2\ ,$$

where all the theta functions are evaluated at (p_1, p_2, p_3).

This should be viewed as an analogue of the classical Thomae's formula for hyperelliptic curves over the complex numbers. We are now able to state the theorem concerning the period doubling of the Richelot isogeny.

Theorem 4.15. *Let X be a Mumford curve, given by the equation over K*

$$X : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

with λ, μ and ν distinct p-adic numbers such that

$$\lambda \equiv \infty \mod \pi\ , \quad \mu \equiv 0 \mod \pi \quad \textit{and} \quad \nu \equiv 1 \mod \pi\ .$$

Denote the half periods of X by p_1, p_2, $p_3 \in \mathbb{C}_p$. Apply the Bost-Mestre arithmetic-geometric mean to X using the canonical quadratic splitting and denote the resulting curve by $\widetilde{X}$. Then the half periods $\widetilde{p}_1$, $\widetilde{p}_2$ and $\widetilde{p}_3$ of $\widetilde{X}$ are given by p_1^2, p_2^2 and p_3^2 respectively. More precisely, $\widetilde{X}$ can be reduced to the form

$$\widetilde{X} : y^2 = x(x-1)(x-\widetilde{\lambda})(x-\widetilde{\mu})(x-\widetilde{\nu})$$

such that

$$\widetilde{\lambda} = \left(1 - \left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_6(p_1^2,p_2^2,p_3^2)}{\theta_2(p_1^2,p_2^2,p_3^2)\theta_7(p_1^2,p_2^2,p_3^2)}\right)^2\right)^{-1},$$
$$\widetilde{\mu} = 1 - \left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_9(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_8(p_1^2,p_2^2,p_3^2)}\right)^2,$$
$$\widetilde{\nu} = \left(\frac{\theta_2(p_1^2,p_2^2,p_3^2)\theta_4(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_5(p_1^2,p_2^2,p_3^2)}\right)^2.$$

Proof. The method used here is identical to that of Theorem 2.27. However, over $\mathbb{C}$ there was no canonical way to partition the roots and so we chose an ordering which was the most convenient. Here we need to take the pairs of roots in the same p-adic discs, which explains some minor changes in the algebra involved (that is also to say, had we chosen a different ordering of roots over $\mathbb{C}$, this would be a corollary of Theorem 2.27!).

Apply the Bost-Mestre algorithm to five roots of X by letting

$$P = x(x-\mu)\ , \quad Q = (x-1)(x-\nu)\ , \quad \text{and} \quad R = x - \lambda\ .$$

Therefore the equation of X' is given by

$$\widetilde{X} : y^2 = (x-a)(x-b)(x-c)(x-d)(x-e)(x-f)\ ,$$

where

$$a = \lambda + \sqrt{(\lambda-1)(\lambda-\nu)}\ ,$$
$$b = \lambda + \sqrt{\lambda(\lambda-\mu)}\ ,$$
$$c = \lambda - \sqrt{\lambda(\lambda-\mu)}\ ,$$
$$d = \frac{-\nu + \sqrt{\nu(\mu-1)(\mu-\nu)}}{\mu-\nu-1}\ ,$$
$$e = \frac{-\nu - \sqrt{\nu(\mu-1)(\mu-\nu)}}{\mu-\nu-1}\ ,$$
$$f = \lambda - \sqrt{(\lambda-1)(\lambda-\nu)}\ .$$

Note that we have

$$\begin{aligned} a \equiv b \equiv \infty \mod \pi \ , \\ c \equiv d \equiv 0 \mod \pi \ , \\ e \equiv f \equiv 1 \mod \pi \ , \end{aligned}$$

since for example

$$|a|_\pi = \left|\lambda + \sqrt{(\lambda-1)(\lambda-\nu)}\right|_\pi > 1 \ .$$

To transform $\widetilde{X}$ into our desired form, we take the transformation

$$x' = \frac{x-d}{x-b} \cdot \frac{f-b}{f-d} \quad \text{or} \quad x = \frac{(f-d)bx' - (f-b)d}{(f-d)x' - (f-b)} \ ,$$

which gives

$$\widetilde{X} : y'^2 = x'(x'-1)\left(x' - \frac{(a-d)(f-b)}{(a-b)(f-d)}\right)\left(x' - \frac{(c-d)(f-b)}{(c-b)(f-d)}\right)\left(x' - \frac{(e-d)(f-b)}{(e-b)(f-d)}\right) \ .$$

It suffices to show that

$$\frac{(a-d)(f-b)}{(a-b)(f-d)} = \left(1 - \left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_6(p_1^2,p_2^2,p_3^2)}{\theta_2(p_1^2,p_2^2,p_3^2)\theta_7(p_1^2,p_2^2,p_3^2)}\right)^2\right)^{-1} , \tag{4.1}$$

$$\frac{(c-d)(f-b)}{(c-b)(f-d)} = 1 - \left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_9(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_8(p_1^2,p_2^2,p_3^2)}\right)^2 , \tag{4.2}$$

$$\frac{(e-d)(f-b)}{(e-b)(f-d)} = \left(\frac{\theta_2(p_1^2,p_2^2,p_3^2)\theta_4(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_5(p_1^2,p_2^2,p_3^2)}\right)^2 . \tag{4.3}$$

As in the complex case, this amounts to some (even more!) tedious manipulation of theta functions. We first do some simple calculations by substituting

$$\lambda = \left(1 - \left(\frac{\theta_3\theta_6}{\theta_2\theta_7}\right)^2\right)^{-1} , \quad \mu = 1 - \left(\frac{\theta_3\theta_9}{\theta_1\theta_8}\right)^2 \quad \text{and} \quad \nu = \left(\frac{\theta_2\theta_4}{\theta_1\theta_5}\right)^2$$

and using the theta relations to obtain

$$\begin{aligned}
1+\nu-\mu &= \frac{\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2}{\theta_1^2\theta_5^2\theta_8^2}\ ,\\
\lambda(\lambda-\mu) &= \frac{\theta_2^2\theta_3^2\theta_7^2[\theta_1^2\theta_6^2\theta_8^2+\theta_2^2\theta_7^2\theta_9^2-\theta_3^2\theta_6^2\theta_9^2]}{\theta_1^2\theta_8^2[\theta_2^2\theta_7^2-\theta_3^2\theta_6^2]^2} = \frac{\theta_0^2\theta_2^2\theta_3^2\theta_7^4}{p_1^2\theta_1^2\theta_5^4\theta_8^4}\ ,\\
\lambda-\nu-\lambda\mu+\lambda\nu &= \frac{\theta_2^2\theta_3^2(\theta_4^2\theta_6^2\theta_8^2+\theta_5^2\theta_7^2\theta_9^2)}{\theta_1^2\theta_5^2\theta_8^2[\theta_2^2\theta_7^2-\theta_3^2\theta_6^2]} = \frac{\theta_2^2\theta_3^2(\theta_4^2\theta_6^2\theta_8^2+\theta_5^2\theta_7^2\theta_9^2)}{p_1\theta_1^2\theta_5^4\theta_8^4}\left(=\frac{\theta_0^2\theta_2^2\theta_3^2(\theta_7^4-\theta_6^4)}{p_1^2\,\theta_1^2\theta_5^4\theta_8^4}\right)\ ,\\
\sqrt{(\lambda-1)(\lambda-\nu)} &= \sqrt{\frac{\theta_2^2\theta_3^2\theta_6^2[\theta_1^2\theta_5^2\theta_7^2+\theta_3^2\theta_4^2\theta_6^2-\theta_2^2\theta_4^2\theta_7^2]}{\theta_1^2\theta_5^2[\theta_2^2\theta_7^2-\theta_3^2\theta_6^2]^2}} = \frac{\theta_0\theta_2\theta_3\theta_6^2}{p_1\theta_1\theta_5^2\theta_8^2}\ ,\\
\sqrt{\nu(\mu-1)(\mu-\nu)} &= \sqrt{\frac{\theta_2^2\theta_3^2\theta_4^2\theta_9^2[\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2-\theta_1^2\theta_5^2\theta_8^2]}{\theta_1^6\theta_5^4\theta_8^4}} = \frac{\theta_0\theta_2\theta_3\theta_4^2\theta_9^2}{\theta_1^3\theta_5^2\theta_8^2}\ ,\\
\sqrt{\lambda(\lambda-\mu)(\lambda-\nu)(\lambda-1)} &= \sqrt{\frac{\theta_2^4\theta_3^4\theta_6^2\theta_7^2}{\theta_1^4\theta_5^2\theta_8^2}\left(\frac{[\theta_1^2\theta_6^2\theta_8^2+\theta_2^2\theta_7^2\theta_9^2-\theta_3^2\theta_6^2\theta_9^2][\theta_1^2\theta_5^2\theta_7^2+\theta_3^2\theta_4^2\theta_6^2-\theta_2^2\theta_4^2\theta_7^2]}{[\theta_2^2\theta_7^2-\theta_3^2\theta_6^2]^4}\right)}\\
&= \frac{\theta_0^2\theta_2^2\theta_3^2\theta_6^2\theta_7^2}{p_1^2\theta_1^2\theta_5^4\theta_8^4}\ .
\end{aligned}$$

Splitting up the left hand side of (4.1) we have

$$\begin{aligned}
\frac{f-b}{a-b} &= \frac{\sqrt{(\lambda-\mu)(\lambda-\nu)}+\sqrt{\lambda(\lambda-\mu)}}{\sqrt{(\lambda-\mu)(\lambda-\nu)}-\sqrt{\lambda(\lambda-\mu)}}\\
&= 1+\frac{2\lambda(\lambda-\mu)+2\sqrt{\lambda(\lambda-\mu)(\lambda-\nu)(\lambda-1)}}{\lambda\mu-\lambda\nu-\lambda+\nu}
\end{aligned}$$

and hence by the above we have

$$\begin{aligned}
\frac{f-b}{a-b} &= 1-\frac{2\theta_0^2\theta_7^4+2\theta_0^2\theta_6^2\theta_7^2}{p_1(\theta_4^2\theta_6^2\theta_8^2+\theta_5^2\theta_7^2\theta_9^2)}\\
&= \frac{[p_1\theta_5^2\theta_9^2-\theta_0^2\theta_7^2]\theta_7^2+p_1\theta_4^2\theta_6^2\theta_8^2-\theta_0^2\theta_7^4-2\theta_0^2\theta_6^2\theta_7^2}{[p_1\theta_5^2\theta_7^2\theta_9^2+\theta_1^2\theta_6^2\theta_7^2]+[p_1\theta_4^2\theta_6^2\theta_8^2-\theta_1^2\theta_6^2\theta_7^2]}\\
&= \frac{[p_1\theta_4^2\theta_8^2-\theta_1^2\theta_7^2]\theta_6^2-\theta_0^2\theta_7^4-2\theta_0^2\theta_6^2\theta_7^2}{\theta_0^2\theta_7^4-\theta_0^2\theta_6^4}\\
&= \frac{-\theta_6^4-\theta_7^4-2\theta_6^2\theta_7^2}{\theta_7^4-\theta_6^4}\\
&= \frac{\theta_7^2+\theta_6^2}{\theta_7^2-\theta_6^2}\ .
\end{aligned}$$

For the other term we have

$$\begin{aligned}\frac{a-d}{f-d} &= \frac{(1+\nu-\mu)\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu}{(\mu-\nu-1)\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu} \\ &= 1+2\,\frac{(1+\nu-\mu)\sqrt{(\lambda-1)(\lambda-\nu)}}{(\mu-\nu-1)\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu} \\ &= 1+2\,\frac{p_1\theta_6^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)}{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1(\theta_2^2\theta_4^2\theta_6^2\theta_8^2+\theta_3^2\theta_5^2\theta_6^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}\ .\end{aligned}$$

Therefore combining everything together we get

$$\begin{aligned}\frac{(a-d)(f-b)}{(a-b)(f-d)} &= \left(1+2\,\frac{p_1\theta_6^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)}{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1(\theta_2^2\theta_4^2\theta_6^2\theta_8^2+\theta_3^2\theta_5^2\theta_6^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}\right)\left(\frac{\theta_7^2+\theta_6^2}{\theta_7^2-\theta_6^2}\right) \\ &= 1+2\frac{\theta_6^2(p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2+p_1(\theta_2^2\theta_4^2\theta_7^2\theta_8^2+\theta_3^2\theta_5^2\theta_7^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4))}{\left(p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1(\theta_2^2\theta_4^2\theta_6^2\theta_8^2+\theta_3^2\theta_5^2\theta_6^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)\right)(\theta_7^2-\theta_6^2)} \\ &= 1+2\,\frac{\Theta_1}{\Theta_2}\ ,\end{aligned}$$

where Θ_1 and Θ_2 denote the numerator and denominator in the expression respectively.

Now on the right hand side we have (where θ_i without the arguments is assumed to be evaluated at (p_1,p_2,p_3) for notational simplicity)

$$\begin{aligned}\left(1-\left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_6(p_1^2,p_2^2,p_3^2)}{\theta_2(p_1^2,p_2^2,p_3^2)\theta_7(p_1^2,p_2^2,p_3^2)}\right)^2\right)^{-1} &= \frac{\theta_2(p_1^2,p_2^2,p_3^2)^2\theta_7(p_1^2,p_2^2,p_3^2)^2}{p_1^2\theta_5(p_1^2,p_2^2,p_3^2)^2\theta_8(p_1^2,p_2^2,p_3^2)^2} \\ &= \frac{(\theta_0\theta_2+\theta_1\theta_3)(\theta_0^2+\theta_1^2-\theta_2^2-\theta_3^2)}{(\theta_0^2-\theta_1^2-\theta_2^2+\theta_3^2)(\theta_0\theta_2-\theta_1\theta_3)} \\ &= 1+2\frac{(\theta_0\theta_3+\theta_1\theta_2)(\theta_0\theta_1-\theta_2\theta_3)}{(\theta_0^2-\theta_1^2-\theta_2^2+\theta_3^2)(\theta_0\theta_2-\theta_1\theta_3)} \\ &= 1+2\,\frac{\Theta_3}{\Theta_4}\ .\end{aligned}$$

Therefore to complete the argument it amounts to showing that

$$\Theta_1\Theta_4-\Theta_2\Theta_3=0$$

and we proceed as in Theorem 2.27 using Maple. However, here we aim to eliminate all θ_4^2, θ_5^2, θ_8^2 and θ_9^2 using the formula

$$\theta_4^2\theta_5^2=\frac{1}{p_2}\left(\theta_0^2\theta_3^2-\theta_1^2\theta_2^2\right)\ ,$$

which leaves us with a homogenous polynomial of degree 14 in the six remaining theta functions with roughly 80 terms. Lowering the powers of θ_6 and θ_7 via

$$p_2p_3\,\theta_6^2\theta_7^2 = \theta_0^2\theta_1^2 - \theta_2^2\theta_3^2 \quad \text{and} \quad p_2p_3\left(\theta_6^4+\theta_7^4\right) = \theta_0^4+\theta_1^4-\theta_2^4-\theta_3^4$$

gives a factorisation of the form

$$\frac{1}{p_2p_3}F_1(\theta_0,\theta_1,\theta_2,\theta_3,\theta_6,\theta_7)(p_2p_3\,\theta_6^2\theta_7^2-\theta_0^2\theta_1^2+\theta_2^2\theta_3^2)\ ,$$

where F_1 is a degree 10 polynomial with eight terms. But we know from the theta identities that the second bracket vanishes and thus this proves (4.1).

For the left hand side of (4.2) we have

$$\frac{f-b}{c-b} = \frac{1}{2}\frac{\sqrt{\lambda(\lambda-\mu)(\lambda-\nu)(\lambda-1)}+\lambda(\lambda-\mu)}{\lambda(\lambda-\mu)} = \frac{1}{2}\frac{\theta_6^2+\theta_7^2}{\theta_7^2}$$

and

$$\begin{aligned}\frac{c-d}{f-d} &= \frac{(\mu-\nu-1)\sqrt{\lambda(\lambda-\mu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu}{(\mu-\nu-1)\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu}\\ &= \frac{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1\theta_7^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1\theta_6^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}\ .\end{aligned}$$

The right hand side simplifies to

$$\begin{aligned}1-\left(\frac{\theta_3(p_1^2,p_2^2,p_3^2)\theta_9(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_8(p_1^2,p_2^2,p_3^2)}\right)^2 &= -\frac{p_2^2\theta_4(p_1^2,p_2^2,p_3^2)^2\theta_7(p_1^2,p_2^2,p_3^2)^2}{\theta_1(p_1^2,p_2^2,p_3^2)^2\theta_8(p_1^2,p_2^2,p_3^2)^2}\\ &= -\frac{(\theta_0\theta_3-\theta_1\theta_2)(\theta_0^2+\theta_1^2-\theta_2^2-\theta_3^2)}{2(\theta_0\theta_1+\theta_2\theta_3)(\theta_0\theta_2-\theta_1\theta_3)}\ .\end{aligned}$$

Doing the same computation on the difference after cross multiplying gives, once again, a factorisation of the form

$$\frac{1}{p_2p_3}F_2(\theta_0,\theta_1,\theta_2,\theta_3,\theta_6,\theta_7)(p_2p_3\theta_6^2\theta_7^2-\theta_0^2\theta_1^2+\theta_2^2\theta_3^2)$$

which proves (4.2).

Finally for (4.3) we have, on the left,

$$\begin{aligned}\frac{f-b}{e-b} &= \frac{(\mu-\nu-1)(\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\lambda(\lambda-\mu)})}{(\mu-\nu-1)\sqrt{\lambda(\lambda-\mu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}-\lambda+\nu+\lambda\mu-\lambda\nu} \\ &= -\frac{p_1(\theta_6^2+\theta_7^2)(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)}{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1\theta_7^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)-\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}\end{aligned}$$

and

$$\begin{aligned}\frac{e-d}{f-d} &= \frac{2\sqrt{\nu(\lambda-1)(\lambda-\nu)}}{(\mu-\nu-1)\sqrt{(\lambda-1)(\lambda-\nu)}+\sqrt{\nu(\mu-1)(\mu-\nu)}+\lambda-\nu-\lambda\mu+\lambda\nu} \\ &= \frac{2p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2}{p_1^2\theta_4^2\theta_5^2\theta_8^2\theta_9^2-p_1\theta_6^2(\theta_2^2\theta_4^2\theta_8^2+\theta_3^2\theta_5^2\theta_9^2)+\theta_0\theta_1\theta_2\theta_3(\theta_7^4-\theta_6^4)}\ .\end{aligned}$$

And on the other hand we have

$$\left(\frac{\theta_2(p_1^2,p_2^2,p_3^2)\theta_4(p_1^2,p_2^2,p_3^2)}{\theta_1(p_1^2,p_2^2,p_3^2)\theta_5(p_1^2,p_2^2,p_3^2)}\right)^2 = \frac{2(\theta_0\theta_2+\theta_1\theta_3)(\theta_0\theta_3-\theta_1\theta_2)}{(\theta_0\theta_1+\theta_2\theta_3)(\theta_0^2-\theta_1^2-\theta_2^2+\theta_3^2)}\ .$$

Applying once again the same procedure yields a slightly different result:

$$\frac{2}{p_2^2p_3^2}(\theta_0\theta_2+\theta_1\theta_3)(\theta_0\theta_3-\theta_1\theta_2)F_3(\theta_0,\theta_1,\theta_2,\theta_3)(p_2p_3(\theta_6^4+\theta_7^2)-\theta_0^4-\theta_1^4+\theta_2^4+\theta_3^4)\ ,$$

where F_3 (only in four variables!) is a degree 12 polynomial with 12 terms. But once again the last term vanishes and thus this concludes the proof. □

4.5 Arithmetic in the Jacobian

The last part of our work requires explicit computations inside the Jacobian, therefore we digress slightly here and describe the basic principles of arithmetic in the Jacobian following [Lei05] and [MWZ96].

Adding points in the Jacobian is most simply done by considering the points as divisors. Let X be a genus g hyperelliptic curve with a $2g+1$ degree model $y^2=f(x)$ with a unique point at ∞. We say that a divisor $D\in \mathrm{Div}^0(X)$ is *semi-reduced* if it is of the form

$$D=\left[\sum_{P_i\in C} m_iP_i-\left(\sum_i m_i\right)\infty\right]$$

where we have $m_i\geq 0$ and $P_i\neq\infty$ for all i. Furthermore, if P_i is in the support of D,

then the hyperelliptic involution $\overline{P_i}$ of the point does not lie in the support unless P_i is a Weierstrass point, in which case $m_i = 1$.

Proposition 4.16. *For all $D \in \mathrm{Div}^0(X)$, there exists a semi-reduced degree 0 divisor D' such that D and D' are linearly equivalent.*

A proof can be found in Section 5 of [MWZ96]. If X has an even degree model of degree $2g+2$, then there are two points at infinity, say ∞_1 and ∞_2. In this case there are multiple treatments in the literature. One method is to allow ∞_1 to be in the support of a semi-reduced divisor (and ∞_2 remains as the distinguished point). Here instead we use a *balanced* point at infinity given by

$$\infty = \frac{1}{2}(\infty_1 + \infty_2) \ .$$

The reason is to match the treatment used by Magma in the computational side of things later. Mumford further simplified this problem by introducing a way to represent semi-reduced divisors as a pair of polynomials. The following is Theorem 42 from [MWZ96]:

Theorem 4.17. *Let*

$$D = \left[\sum_{(x_i,y_i)\in C} m_i(x_i, y_i) - \left(\sum_i m_i \right) \infty \right]$$

be a semi-reduced divisor over a hyperelliptic curve X. Let

$$A(x) = \prod_i (x - x_i)^{m_i}$$

and $B(x)$ be the (unique) polynomial such that

(i) $\deg B < \deg A$,

(ii) $B(x_i) = y_i$ *for all i where* $m_i \neq 0$,

(iii) $A(x)$ *divides* $(B(x)^2 - f(x))$

Then $D = \gcd(\mathrm{Div}(A(x), \mathrm{Div}(B(x) - y))$ and we write $D = [A(x), B(x)]$.

The problem with working with semi-reduced divisors is that they are, in general, not unique in their divisor classes. The solution is to define a subset of these divisors, called *reduced divisors*, where

$$D = \left[\sum_{P_i \in C} m_i P_i - \left(\sum_i m_i \right) \infty \right]$$

with the sum of the m_i's at most the genus g of X.

Theorem 4.18. *For all $D \in \mathrm{Div}^0(C)$, there exists a unique reduced divisor D' such that D and D' are linearly equivalent.*

This is Theorem 47 from [MWZ96]. Therefore for each divisor class in the Jacobian $J(X) = \mathrm{Div}^0(X)/\mathrm{Div}^P(X)$, there exists a unique reduced divisor representative, which is what we will work with from now on.

We quickly sketch in passing how these divisors look in genus 2. Since the order of the points sum to at most 2, non-zero divisors are either of the form $D = [(x_1, y_1) - \infty]$ (i.e. weight 1) or $D' = [(x_1, y_1) + (x_2, y_2) - 2\infty]$ (i.e. weight 2). In the first case the Mumford representation of D is simply $[x - x_1, y - y_1]$ and in the latter case the representation of D' is given by $[(x - x_1)(x - x_2), f(x)]$, where $f(x)$ is the equation of the straight line passing through the two points.

The second advantage of employing these reduced divisors is for doing arithmetic inside the Jacobian. We first describe the group law of the Jacobian, which should be seen as a generalisation of the tangent and chord construction for elliptic curves.

Consider two generic divisors $D = [P_1 + P_2 - 2\infty]$ and $D' = [Q_1 + Q_2 - 2\infty]$ for a curve X defined by $y^2 = f(x)$. Then there exists a unique cubic (counted with multiplicity if any of the four points coincides) that passes through the four points P_1, P_2, Q_1 and Q_2. Now intersecting this cubic with $f(x)$ gives two extra roots, say R_1 and R_2. Then define the sum of D and D' as the involution of these two points, that is,

$$D + D' = \left[\overline{R_1} + \overline{R_2} - 2\infty\right] \ .$$

Explicit formulae can be found in [Lei05]. If one works instead with Mumford representations, the following two algorithms, by Cantor and later generalised by Koblitz, give a simple way to add divisors.

Algorithm 4.19.
Input: Two reduced divisors $D_1 = [A_1, B_1]$ and $D_2 = [A_2, B_2]$.
Ouput: A semi-reduced divisor $D = [A, B]$.

1. *Compute polynomials d_1, e_1 and e_2 using the Euclidean algorithm such that*

$$d_1 = \gcd(A_1, A_2) = e_1 A_1 + e_2 A_2 \ .$$

2. *Compute polynomials d, c_1 and c_2 such that*

$$d = \gcd(d_1, B_1 + B_2) = c_1 d_1 + c_2 (B_1 + B_2) \ .$$

3. *Let $s_1 = c_1 e_1$, $s_2 = c_1 e_2$ and $s_3 = c_2$ such that*

$$d = s_1 A_1 + s_2 A_2 + s_3 (B_1 + B_2) \ .$$

4. *Then $D_1 + D_2 = [A, B]$, where*

$$A = \frac{A_1 A_2}{d^2} \quad \textit{and} \quad B = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3 (B_1 B_2 + f)}{d} \mod A \ .$$

The above algorithm outputs the sum of two divisors which need not be reduced (although it is always semi-reduced). The second algorithm turns this into a reduced divisor.

Algorithm 4.20.
Input: A semi-reduced divisors $D = [A, B]$.
Ouput: A reduced divisor $D' = [A', B']$.

1. *Set*

$$A' = \frac{f - B^2}{A} \quad \textit{and} \quad B' = -B \mod A' \ .$$

2. *If $\deg A' > g$ then let $A = A'$, $B = B'$ and repeat step 1.*

3. *Normalise A' such that its leading coefficient is 1.*

4. *Then $D \sim [A', B']$.*

In genus 2, the degree of the output A in Algorithm 4.19 is at most 4 whence it only takes at most one iteration of Step 1 to reduce it to a reduced divisor. Proofs of these algorithms can be found in [Kob89].

4.6 An Overview of the Strategy

We now have all the necessary tools at our disposal to describe our strategy from the introduction in more detail. Given a totally split curve X_0 of genus 2 with Type B reduction, we consider the Jacobian J_0, and its uniformisation by a Schottky group Γ_0. Using the Bost-Mestre algorithm we obtain X_1 which is isogenous to X_0 and thus inducing a map on the Jacobians $J_1 \longrightarrow J_0$ whose kernel is a $(2,2)$-group. Theorem 4.15 shows that this Richelot isogeny doubles the half periods of X_0, suggesting that this is the right generalisation from genus 1 that we should consider.

We pick an element in the kernel of g_0, the map from $J_1 \longrightarrow J_0$, and lift it by the Richelot isogeny to J_2. After reordering the roots of X_2, repeat the process to desired precision. Then map this up to the uniformisation X_{Γ_n}/Γ_n and then to $(K^\times)^2/H_{\Gamma_n}$, where we treat the map ϕ_n as the degenerate map ϕ_∞ for some sufficiently large n. From there we hope to recover the periods q_i's (or equivalently the half-periods p_i's). The following diagram summarises our strategy:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & (K^\times)^2/H_n & \longrightarrow & \cdots & \xrightarrow{f_1} & (K^\times)^2/H_1 & \xrightarrow{f_0} & (K^\times)^2/H_0 \\
 & & \phi_n \downarrow \wr & & & & \phi_1 \downarrow \wr & & \phi_0 \downarrow \wr \\
\cdots & \longrightarrow & J_n & \longrightarrow & \cdots & \xrightarrow{g_1} & J_1 & \xrightarrow{g_0} & J_0 \\
 & & \uparrow & & & & \uparrow & & \uparrow \\
 & & X_n & & & & X_1 & & X_0
\end{array}$$

Given the equation of X_0, the algorithm described in Section 4.3 gives us the equations of all the successive curves X_i's. Section 4.4 provides the framework to lift the divisors along the chain of Jacobians J_i's. Here we will devote the remaining of our efforts to lifting the divisors only, but we will provide some insights at the end on how the maps ϕ_i's should look like and how one would go about inverting them.

4.7 Kummer Surfaces

One main requirement of the strategy is to verify that the maps f_i's are the identity maps. We will get evidence for this by returning to the complex situation and studying the theory of Kummer surfaces. We will also explain why the situation over $\mathbb{C}$ should also apply for p-adic fields. Our investigation also led us to an alternative method to lift the Richelot isogeny – by descending onto the Kummer surface and try to work with isogenous Kummer

instead, and thus avoid directly pulling back along the g_i's which seems to be computationally difficult. This was not the method we employed ultimately, for reasons which will become apparent, but nonetheless we include it for the reader's interest.

We begin with a quick introduction to Kummer surfaces following [Gau07]. Note that theta functions in this section are now the ones previously defined in Section 2.5, not the p-adic ones in Section 4.3.1. Also, we work not only with theta constants here, and our notations should hopefully be clear enough not to cause confusion. Fix $\Omega \in \mathbb{H}_2$. Then the Kummer surface associated to Ω, denoted $\mathcal{K}(\Omega)$ or just $\mathcal{K}$, is the image of the map $\varphi : \mathbb{C}^2 \longrightarrow \mathbb{P}^3(\mathbb{C})$ where

$$\varphi(\mathbf{z}) = [\theta_0(2\mathbf{z}) : \theta_3(2\mathbf{z}) : \theta_2(2\mathbf{z}) : \theta_1(2\mathbf{z})]$$

(note [Gau07] uses a different labelling of the theta functions). This map is well defined since the four theta functions never vanish simultaneously. It is a quartic, irreducible nodal surface of dimension 2 with a maximal possible number of 16 double points. It can also be realised as the quotient of the Jacobian of a genus 2 hyperelliptic curve by the involution $(x \mapsto -x)$, for example see Chapter 3 of [CF96].

It is also interesting to note that the map defining the Kummer surface only utilises θ_0, θ_1, θ_2 and θ_3. Upon looking at the correspondence of p-adic theta functions in Proposition 4.13, one realises that their p-adic analogues do not involve any extra terms unlike the rest of the theta functions. This gives us extra confidence that if the maps f_i's are indeed the identity maps over $\mathbb{C}$, the same reasoning should carry over to the p-adic world.

Our interest here begins with the observation that a Kummer surface can be parametrised by the theta constants

$$a = \theta_0(0, \Omega) \ , \quad b = \theta_3(0, \Omega) \ , \quad c = \theta_2(0, \Omega) \ , \quad d = \theta_1(0, \Omega)$$

and

$$A = \theta_0(0, 2\Omega) \ , \quad B = \theta_5(0, 2\Omega) \ , \quad C = \theta_9(0, 2\Omega) \ , \quad D = \theta_7(0, 2\Omega) \ .$$

Now let $[x : y : z : t] \in \mathcal{K}$, that is,

$$x = \lambda\theta_0(\mathbf{z}, \Omega) \ , \quad y = \lambda\theta_3(\mathbf{z}, \Omega) \ , \quad z = \lambda\theta_2(\mathbf{z}, \Omega) \ , \quad t = \lambda\theta_1(\mathbf{z}, \Omega)$$

for some $\mathbf{z} \in \mathbb{C}^2$ and $\lambda \in \mathbb{C}^\times$. Then a projective equation of $\mathcal{K}$ is given by

$$(x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2) - G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) = 0 \ ,$$

where

$$\begin{aligned} E &= 256\,\frac{abcdA^2B^2C^2D^2}{(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2)} \ , \\ F &= \frac{a^4 - b^4 - c^4 + d^4}{(a^2d^2 - b^2c^2)} \ , \\ G &= \frac{a^4 - b^4 + c^4 - d^4}{(a^2c^2 - b^2d^2)} \ , \\ H &= \frac{a^4 + b^4 - c^4 - d^4}{(a^2b^2 - c^2d^2)} \ . \end{aligned}$$

Now since it is possible to express A, B, C and D linearly in terms of a^2, b^2, c^2 and d^2 (for example see Theorem 2.7), the equation of $\mathcal{K}(\Omega)$ is essentially determined entirely by a, b, c and d. We will gloss over the theory of doing arithmetic inside the Kummer surface; see [Gau07] for algorithms for doubling and addition in the Kummer surface. Our focus is mainly in passing from the Jacobian to the Kummer surface and maps between isogenous Kummer surfaces. We first describe a method to lift points from the Kummer surface to the Jacobian.

Fix a period matrix $\Omega \in \mathbb{H}_2$ associated to the hyperelliptic curve given by

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu) \ ,$$

where

$$\lambda = \frac{\theta_0(0)^2\theta_2(0)^2}{\theta_3(0)^2\theta_1(0)^2} \ , \quad \mu = \frac{\theta_0(0)^2\theta_5(0)^2}{\theta_3(0)^2\theta_4(0)^2} \quad \text{and} \quad \nu = \frac{\theta_0(0)^2\theta_5(0)^2}{\theta_3(0)^2\theta_4(0)^2}$$

(note that the notation varies slightly from that in Chapter 2 – all theta functions without the second argument are evaluated at Ω). Compute all the theta constants $\theta_i(0)$. The 16 two-torsion points on $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2)$ are mapped to 16 nodes on $\mathcal{K}(\Omega)$. Since the Kummer surface is the quotient of the Jacobian by the involution $(x \mapsto -x)$, these are the only points with unique preimages in the Jacobian.

Using the above model for the Kummer surface, these 16 nodes are precisely

$$\begin{array}{llll} (a,b,c,d)\ , & (a,b,-c,-d)\ , & (a,-b,c,-d)\ , & (a,-b,-c,d)\ , \\ (b,a,d,c)\ , & (b,a,-d,-c)\ , & (b,-a,d,-c)\ , & (b,-a,-d,c)\ , \\ (c,d,a,b)\ , & (c,d,-a,-b)\ , & (c,-d,a,-b)\ , & (c,-d,a,-b)\ , \\ (d,c,b,a)\ , & (d,c,-b,-a)\ , & (d,-c,b,-a)\ , & (d,-c,b,-a)\ . \end{array}$$

For the next part we require the six odd theta functions in genus 2 which we omitted in Section 2.5; we briefly define them here without giving their series expansions:

$$\begin{aligned} \theta_{10}(\mathbf{z},\Omega) &= \theta \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}(\Omega)\ , \quad \theta_{11}(\mathbf{z},\Omega) = \theta \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}(\Omega)\ , \\ \theta_{12}(\mathbf{z},\Omega) &= \theta \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}(\Omega)\ , \quad \theta_{13}(\mathbf{z},\Omega) = \theta \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}(\Omega)\ , \\ \theta_{14}(\mathbf{z},\Omega) &= \theta \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}(\Omega)\ , \quad \theta_{15}(\mathbf{z},\Omega) = \theta \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(\Omega)\ . \end{aligned}$$

Now let $P = (x, y, z, t) \in \mathcal{K}$ be a point that is not one of the above nodes. We will compute a pair of polynomials $[U, V]$ which represents the point P inside the Jacobian of the curve. Define

$$u_0 = \lambda \frac{\theta_5(0)^2\theta_{13}(\mathbf{z})^2}{\theta_4(0)^2\theta_{15}(\mathbf{z})^2} \quad \text{and} \quad u_1 = (\lambda - 1)\frac{\theta_7(0)^2\theta_{12}(\mathbf{z})^2}{\theta_4(0)^2\theta_{15}(\mathbf{z})^2} - u_0 - 1\ ,$$

then $U(x) = x^2 + u_1 x + u_0$ is the first component of the Mumford representation. Since $V(x)$ is essentially the line going through the two points represented by the divisor, the roots of $U(x)$ give at most four $V(x)$ (more precisely two pairs of opposite divisors) such that the pair $[U, V]$ lies on the Jacobian. Now explicitly v_0^2 is given by

$$\begin{aligned} v_0^2 = -V_0 \frac{\theta_{13}(\mathbf{z})^2}{\theta_{15}(\mathbf{z})^6} \Big(& V_1\theta_9(\mathbf{z})^2\theta_{11}(\mathbf{z})^2 + V_2\theta_8(\mathbf{z})^2\theta_{10}(\mathbf{z})^2 + \\ & V_3\big(\theta_0(\mathbf{z})^2\theta_2(\mathbf{z})^2 + \theta_1(\mathbf{z})^2\theta_3(\mathbf{z})^2\big) - V_4\theta_0(\mathbf{z})\theta_1(\mathbf{z})\theta_2(\mathbf{z})\theta_3(\mathbf{z})\Big)\ , \end{aligned}$$

where

$$\begin{aligned}
V_0 &= \frac{\theta_0(0)^4\theta_2(0)^4\theta_5(0)^2}{\theta_1(0)^6\theta_3(0)^6\theta_4(0)^6} \ , \\
V_1 &= \theta_2(0)^2\theta_3(0)^2\theta_8(0)^4 \ , \\
V_2 &= \theta_0(0)^2\theta_1(0)^2\theta_9(0)^4 \ , \\
V_3 &= 2\theta_0(0)^2\theta_1(0)^2\theta_2(0)^2\theta_3(0)^2 \ , \\
V_4 &= 2\theta_0(0)\theta_1(0)\theta_2(0)\theta_3(0)\left(\theta_0(0)^2\theta_2(0)^2 + \theta_1(0)^2\theta_3(0)^2\right) \ .
\end{aligned}$$

Finally, it is easier to compute v_1 from the fact that $U(x)$ divides $V(x)^2 - f(x)$. This means that given a point $P \in \mathcal{K}(\Omega)$, one is only able to compute a divisor $[U, V]$ up to a sign choice (from the square root of v_0^2). This is to be expected, since the Jacobian is a degree 2 cover of the Kummer surface. Note that it is possible, in very few exceptional cases, for the map to be undefined (if the theta constants or $\theta_{15}(\mathbf{z})$ vanish) but this almost never happens.

Recall the Richelot isogeny between the Jacobian of two isogenous hyperelliptic curves of genus 2. We now study how this map translates onto the Kummer surfaces.

We first consider two hyperelliptic curves, X_1 and X_2, which are isogenous curves related via the arithmetic-geometric mean; then as seen in Theorem 2.27, their period matrices are Ω and 2Ω respectively for some $\Omega \in \mathbb{H}_2$. By starting with some $\mathbf{z} \in \mathbb{C}^2$, one can map it to a point in the Kummer surface $\mathcal{K}(\Omega)$ via the theta functions, then further onto the Jacobian by the map described in the previous section (technically one may bypass the Kummer surface since the map from $\mathcal{K}(\Omega)$ to $J(X_1)$ is defined by theta functions and simply takes $\mathbf{z}$ as the argument). Denote this divisor $D_1 \in J(X_1)$. By the dual Richelot isogeny $\hat{\phi}$, one may push this point onto the Jacobian of X_2.

Now define $f_1 : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ simply by $f_1(\mathbf{z}) = 2\mathbf{z}$ and denote the corresponding divisor in $J(X_2)$ by D_2. We conjecture (with a lot of numerical evidence) that inside $J(X_2)$ one has

$$D_2 \equiv \hat{\phi}(D_1) \ ;$$

presumably one might prove this using theta identities as in Chapter 2.

That is to say, we have the following diagram:

$$\begin{array}{ccc} J(X_1) & \xrightarrow{\hat{\phi}} & J(X_2) \\ \uparrow & & \uparrow \\ \mathcal{K}(\Omega) & \longrightarrow & \mathcal{K}(2\Omega) \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ \mathbb{C}^2 & \xrightarrow{f_1} & \mathbb{C}^2 \end{array}$$

Next, consider the composite of ϕ with $\hat{\phi}$. We have also seen in Chapter 2 that

$$\phi \circ \hat{\phi}(D) = 2D$$

for all $D \in J(X_1)$. Therefore it follows immediately that the map f_2 in the following diagram must be the identity map on $\mathbb{C}^2$:

$$\begin{array}{ccccc} J(X_1) & \xrightarrow{\hat{\phi}} & J(X_2) & \xrightarrow{\phi} & J(X_1) \\ \uparrow & & \uparrow & & \uparrow \\ \mathcal{K}(\Omega) & \longrightarrow & \mathcal{K}(2\Omega) & \xrightarrow{g} & \mathcal{K}(\Omega) \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ \mathbb{C}^2 & \xrightarrow[f_1]{} & \mathbb{C}^2 & \xrightarrow[f_2]{} & \mathbb{C}^2 \end{array}$$

We should pause here and stress the importance of this observation – assuming our conjecture that the diagram above commutes. It is in line with the diagram in genus 1 (see Section 3.2 or the beginning of this chapter) in the sense that the maps between $\overline{K}^*/q^{2^n\mathbb{Z}}$ and $\overline{K}^*/q^{2^{n-1}\mathbb{Z}}$ were induced by the identity maps. This gives more confidence that our strategy is the right method in genus 2.

The final map we are interested in is the map g between the two isogenous Kummer surfaces. By definition we have

$$g([\theta_0(\mathbf{z}, 2\Omega) : \theta_3(\mathbf{z}, 2\Omega) : \theta_2(\mathbf{z}, 2\Omega) : \theta_1(\mathbf{z}, 2\Omega)]) = [\theta_0(\mathbf{z}, \Omega) : \theta_3(\mathbf{z}, \Omega) : \theta_2(\mathbf{z}, \Omega) : \theta_1(\mathbf{z}, \Omega)]$$

and therefore an algebraic equation for g can be computed using the various well-known theta identities. More explicitly, by using the Frobenius theta formula one may obtain four linear equations involving only $\theta_i(\mathbf{z}, \Omega)$ on the left and $\theta_i(\mathbf{z}, 2\Omega)^2$ on the right (and where

all the coefficients are theta constants). This gives the following matrix equation

$$M \begin{pmatrix} \theta_0(\mathbf{z},\Omega) \\ \theta_3(\mathbf{z},\Omega) \\ \theta_2(\mathbf{z},\Omega) \\ \theta_1(\mathbf{z},\Omega) \end{pmatrix} = \overline{M} \begin{pmatrix} \theta_0(\mathbf{z},2\Omega)^2 \\ \theta_3(\mathbf{z},2\Omega)^2 \\ \theta_2(\mathbf{z},2\Omega)^2 \\ \theta_1(\mathbf{z},2\Omega)^2 \end{pmatrix} ,$$

where the matrices are given by

$$M = \frac{1}{4} \begin{pmatrix} \theta_0(\Omega) & \theta_3(\Omega) & \theta_2(\Omega) & \theta_1(\Omega) \\ \theta_0(\Omega) & \theta_3(\Omega) & -\theta_2(\Omega) & -\theta_1(\Omega) \\ \theta_0(\Omega) & -\theta_3(\Omega) & \theta_2(\Omega) & -\theta_1(\Omega) \\ \theta_0(\Omega) & -\theta_3(\Omega) & -\theta_2(\Omega) & \theta_1(\Omega) \end{pmatrix}$$

and

$$\overline{M} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -\frac{\theta_7(2\Omega)^2\theta_9(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & -\frac{\theta_6(2\Omega)^2\theta_8(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_7(2\Omega)^2\theta_8(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_6(2\Omega)^2\theta_9(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} \\ -\frac{\theta_5(2\Omega)^2\theta_7(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_4(2\Omega)^2\theta_7(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & -\frac{\theta_4(2\Omega)^2\theta_6(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_5(2\Omega)^2\theta_6(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} \\ -\frac{\theta_5(2\Omega)^2\theta_9(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_4(2\Omega)^2\theta_9(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & \frac{\theta_5(2\Omega)^2\theta_8(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} & -\frac{\theta_4(2\Omega)^2\theta_8(2\Omega)^2}{\theta_5(2\Omega)^4-\theta_6(2\Omega)^4} \end{pmatrix} .$$

These are all theta constants evaluated at $\mathbf{z} = 0$. Therefore to go between $\mathcal{K}(2\Omega)$ and $\mathcal{K}(\Omega)$ (or vice versa) one may compute the inverses of the matrices M or $\overline{M}$ as needed. The 4-to-1 nature of the Richelot isogeny is reflected in the choices of square roots.

The computations involved are relatively simple and can be iterated easily. However, the obvious downfall of this is that it relies on the theta constants (which themselves depend on Ω). It might be possible, for example as in [CF96], to use a different model of the Kummer surface that avoids these theta constants. Using the language of tropes, [CF96] is able to write the Kummer surface as

$$K = Q^2 - \rho L_1 L_2 L_3 L_4 ,$$

where K is a quartic form, Q is a quadratic form, L_i's are linear terms and ρ is a rational number. The isogenous Kummer surface has a similar form and the two surfaces are connected by a system of equations with coefficients from the defining equations of the Richelot

isogeny. However, there are still details missing and some calculations, as the authors noted, are fairly involved. As such we will not pursue this thought any further.

4.8 Lifting the Richelot Isogeny

If ϕ denotes the Richelot isogeny and $\hat{\phi}$ its dual, then we know that $\phi \circ \hat{\phi} = [2]$ on $J(X)$. So if we want to solve the equation

$$\phi([(u_1, v_1) + (u_2, v_2)]) = [(x_1, y_1) + (x_2, y_2)]$$

one could first 'half' the divisor on the right hand side before applying $\hat{\phi}$. The problem of halving a divisor D (i.e. finding D_2 such that $D = 2D_2$) has been previously studied in [MPT15], where they called it *bisection* of D. Note that although they work in finite fields it is clear that the equations translate to any field such as $\mathbb{C}$ or $\mathbb{Q}_p$.

It is of course also possible to first apply the dual isogeny before halving it. Computationally both methods are similar in terms of complexity and feasibility, but as we will see, halving a divisor yeilds 16 answers in general and one then has to deduce which four are the preimages we want. In halving the divisor first, these 16 bisections are then mapped onto only four preimages by the 4-to-1 nature of the Richelot isogeny.

The idea is to 'dereduce' a divisor by reversing Cantor's addition algorithm (Algorithm 4.19 and 4.20), that is, first find a divisor that reduces to the original divisor. Suppose $D = (U(x), V(x))$ is the divisor we wish to half, given in Mumford representation. If $D' = (U'(x), V'(x))$ is a divisor that reduces to D, then we have

$$U(x) = \frac{f(x) - V'(x)^2}{U'(x)} \quad \text{and} \quad V(x) = -V'(x) \mod U(x) \ .$$

Now if $D_1 = (U_1(x), V_1(x))$ satisfies $2D_1 = D$, then one must have

$$U_1(x)^2 = U'(x) \ ,$$

which combined with the fact that $V'(x) = (k_1 x + k_0)U(x) - V(x)$ gives

$$U(x)U'(x) = f(x) - ((k_1 x + k_0)U(x) - V(x))^2 \ .$$

By comparing the coefficients, one obtains six equations in four unknowns. Attempting to solve the system algebraically gives a degree 16 polynomial in k_1, whose coefficients can be found in [MPT15]. Using these values of k_1, one can work out the corresponding values of k_0 and thus $U_1(x)$.

We now give a more detailed description on how to execute the algorithm in practice. Assume for now that the bisection D_1 has weight 2. This implies that we seek a dereduced divisor $U'(x)$ of degree 4, say

$$U'(x) = g_4x^4 + g_3x^3 + g_2x^2 + g_1x + g_0 \ .$$

By comparing $f(x) - ((k_1x + k_0)U(x) - V(x))^2$ and $U(x)U'(x)$ one may choose the g_i's such that their difference is a constant as follows (note that $U(x) = x^2 - sx + p$ and $V(x) = \alpha x + \beta$ for convenience):

$$\begin{aligned}
g_4 &= f_6 - k_1^2 \ , \\
g_3 &= f_5 + sf_6 + sk_1^2 - 2k_0k_1 \ , \\
g_2 &= f_4 + sf_5 + (s^2 - p)f_6 + 2sk_0k_1 - pk_1^2 + 2\alpha k_1 - k_0^2 \ , \\
g_1 &= f_3 + sf_4 + (s^2 - p)f_5 + (s^3 - 2ps)f_6 + sk_0^2 - 2pk_0k_1 + 2(\beta k_1 + \alpha k_0) \ , \\
g_0 &= f_2 + sf_3 + (s^2 - p)f_4 + (s^3 - 2ps)f_5 + (s^4 - 3ps^2 + p^2)f_6 - pk_0^2 + 2\beta k_0 - \alpha^2 \ .
\end{aligned}$$

Next, by equating $U'(x) = U_1(x)^2$ (after normalising $U'(x)$) one immediately gets

$$x^4 + \frac{g_3}{g_4}x^3 + \frac{g_2}{g_4}x^2 + \frac{g_1}{g_4}x + \frac{g_0}{g_4} = x^4 + 2u_1x^3 + (2u_0 + u_1^2)x^2 + 2u_1u_0x + u_0^2$$

and hence one rescales $U'(x)$ to obtain

$$u_1 = \frac{g_3}{2g_4} \quad \text{and} \quad u_0 = \frac{g_2 - g_4u_1^2}{2g_4} \ .$$

Substituting these into the linear and constant terms gives two bivariate polynomials $s_1(k_0, k_1)$ and $s_2(k_0, k_1)$ with

$$s_1 = 8\left(\frac{g_1}{g_4} - 2u_1u_0\right)(k_1^2 - f_6)^3 \quad \text{and} \quad s_2 = 64\left(\frac{g_0}{g_4} - u_0^2\right)(k_1^2 - f_6)^4 \ ,$$

where the denominators are cleared. By construction these two polynomials share a non-constant factor. Hence taking the resultant (i.e. the determinant of the 16×16 Sylvester

matrix) of s_1 and s_2 with respect to k_0 gives a degree 32 polynomial in k_1. In fact this polynomial has a factor of $(k_1^2 - f_6)^8$, so in reality we are working with a degree 16 polynomial. Using these value of k_1 one then computes $\gcd(s_1, s_0)$, whose roots are the value of k_0 we seek. Finally this gives the values of the g_i's and hence the u_i's.

Over an algebraically closed field this degree 16 resultant yields 16 roots. If these roots are distinct then each value corresponds to a distinct divisor. If the resultant has repeated roots, then the degree of the gcd (and hence the number of solutions of k_0) is equal to the multiplicity of that particular k_1. Since the Richelot isogeny is 4-to-1, these 16 divisors map to only four distinct divisors on the dual, which differ by the kernel of the isogeny.

Over non-algebraically closed field such as $\mathbb{F}_p$ or $\mathbb{Q}_p$, such bisection is not always possible, and it becomes an interesting question to ask how many bisections should one expect without extending the field. This has previously been studied and we quote Theorem 1 in [MPT15], which states that for curves we are interested in (that is, with Type B reduction), then one should only expect 4 bisections over $\mathbb{F}_p$.

In practice computing the resultant is easy up to certain precision such as modulo π^{20}. To compute its roots one can first solve the equation modulo π before Hensel lifting them to the desired precision. Note that we assumed two things in the above: that the bisectee D and bisection D_1 are both of weight 2. If D is of weight 1 (that is, $U(x) = x - u$ is linear and $V(x) = v + ax^3 - au^3$ with $(u, v) \in X$ and $a^2 = f_6$), the same method works but the coefficients of the g_i's change as follows:

$$
\begin{aligned}
g_4 &= f_5 + 2ak_1 \ , \\
g_3 &= f_4 + uf_5 - k_1^2 + 2ak_0 \ , \\
g_2 &= f_3 + uf_4 + u^2 f_5 + 2u^3 f_6 + uk_1^2 - 2k_0 k_1 - 2av \ , \\
g_1 &= f_2 + uf_3 + u^2 f_4 + u^3 f_5 + 2u^4 f_6 + 2uk_0 k_1 + 2vk_1 - k_0^2 - 2ak_1 u^3 - 2auv \ , \\
g_0 &= f_1 + uf_2 + u^2 f_3 + u^3 f_4 + u^4 f_5 + 2u^5 f_6 + uk_0^2 + 2vk_0 - 2ak_0 u^3 - 2au^2 v \ .
\end{aligned}
$$

The u_i's remain the same, but the corresponding s_i's become

$$
s_1 = 8\left(\frac{g_1}{g_4} - 2u_1 u_0\right)(f_5 + 2ak_1)^3 \quad \text{and} \quad s_2 = 64\left(\frac{g_0}{g_4} - u_0^2\right)(f_5 + 2ak_1)^4 \ .
$$

Finally, if the bisection D_1 is in fact of weight 1 or 0, then D_1 can be computed by simply

extracting a square root. One simply has to check whether the polynomial $U(x)$ is a square; if it is then D_1 is simply given by the square root of $U(x)$.

We end this section with a slight digression. Since we are only expecting four lifts from the isogeny, one might hope to obtain a quartic by explicitly lifting the map, which would (at least one might hope theoretically) be much simpler than the degree 16 polynomial in the bisection method. We try to mimic the bisection method but work directly on $J(X)$.

Write $y^2 = f(x)$ for the equation of X and work directly with the divisor $[(x_1, y_1) + (x_2, y_2)]$ on X. Recall the explicit description of the Richelot isogeny given by

$$F_z(x) = P(x)U(z) + Q(x)V(z) = -R(x)W(z) - (x - z)^2\Delta \ .$$

Then the same method as the bisection means that we require a cubic $M(x)$ such that

$$f - M^2 = c(x - x_1)(x - x_2)F_{z_1}(x)F_{z_2}(x) \ ,$$

where M is again restricted to be of the form

$$M = (k_1x + k_0)(x - x_1)(x - x_2) - (\alpha x + \beta)$$

with $y = \alpha x + \beta$ denoting the line joining the two points. Comparing coefficients once again give several equations and can be solved. However, from a practical point of view pulling back via bisection seems to give better results in shorter time since the equations involved are much simpler. This is due to the complexity of the coefficients involved in the Richelot isogeny, which makes the solving of the system of equations seemingly impossible in general.

4.9 An Explicit Example: $X_0(23)$

Recall the following diagram:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & (K^\times)^2/H_n & \longrightarrow & \cdots & \xrightarrow{f_1} & (K^\times)^2/H_1 & \xrightarrow{f_0} & (K^\times)^2/H_0 \\
 & & \phi_n \downarrow \wr & & & & \phi_1 \downarrow \wr & & \phi_0 \downarrow \wr \\
\cdots & \longrightarrow & J_n & \longrightarrow & \cdots & \xrightarrow{g_1} & J_1 & \xrightarrow{g_0} & J_0 \\
 & & \uparrow & & & & \uparrow & & \uparrow \\
 & & X_n & & & & X_1 & & X_0
\end{array}$$

Our aim is to take a divisor in the kernel of g_0, pull it back sufficiently far to J_n and then push it to $(K^\times)^2/H_n$ by treating ϕ_n as the degenerate map at infinity. On the lowest row we have Richelot-isogenous curves given by the Bost-Mestre AGM. We believe the maps f_i's to be the identity maps on $(K^\times)^2$ whereas the g_i's are the Richelot isogenies.

We first fix some notations before it turns into a notational nightmare. Denote the totally split curves by X_i's and let J_i's be their corresponding Jacobians for $i \geq 0$. For each i, write the equation of X_i as

$$X_i : T_i y^2 = P_i Q_i R_i$$

with

$$P_i = (x - a_i)(x - a_i'), \quad Q_i = (x - b_i)(x - b_i') \quad \text{and} \quad R_i = (x - c_i)(x - c_i') \ .$$

Note that by Type B-ness we also have

$$a_i \equiv a_i' \equiv \alpha \mod \pi \ , \quad b_i \equiv b_i' \equiv \beta \mod \pi \quad \text{and} \quad c_i \equiv c_i' \equiv \gamma \mod \pi \ ,$$

for three distinct α, β and γ in K. The constants T_i are given by, as in the real case,

$$T_i = \prod_{k=0}^{i} \frac{a_i b_i (e_i + f_i - c_i - d_i) - c_i d_i (e_i + f_i - a_i - b_i) + e_i f_i (c_i + d_i - a_i - b_i)}{(c_i + d_i - a_i - b_i)(e_i + f_i - a_i - b_i)(e_i + f_i - c_i - d_i)}$$

for $i \geq 1$ and $T_0 = 1$ (note the numerator is the determinant Δ_i of the matrix formed by the coefficients of P_i, Q_i and R_i). Define

$$\begin{aligned} U_i &= Q_i' R_i - R_i' Q_i = \varepsilon_1 (x - u_i)(x - u_i') \\ V_i &= R_i' P_i - P_i' R_i = \varepsilon_2 (x - v_i)(x - v_i') \\ W_i &= P_i' Q_i - Q_i' P_i = \varepsilon_3 (x - w_i)(x - w_i') \end{aligned}$$

so that the roots of $U_i V_i W_i$ form the next curve X_{i+1}.

We will demonstrate the algorithm with the modular curve $X_0(23) = X_0$ over $\mathbb{Q}_{23}$. Its equation can be found in [Tei88] (due to Fricke):

$$y^2 = x^6 - 14x^5 + 57x^4 - 106x^3 + 90x^2 - 16x - 19 \ .$$

Over $\mathbb{F}_{23}$ this splits as three pairs of roots

$$y^2 \equiv (x-18)^2(x-21)^2(x-14)^2 \mod 23$$

so that it is indeed totally split of Type B. The roots lie in the extension $\mathbb{Q}_{23}(\pi)$, where π is a root of x^2+23, and Hensel's lemma (or Magma) gives their values up to modulo π^{20}:

$$\begin{aligned}
a_0 &= 26196575459988 + 649618143166\pi \ , \\
a_0' &= 26196575459988 - 649618143166\pi \ , \\
b_0 &= 241232708350 \ , \\
b_0' &= 41266787476103 \ , \\
c_0 &= 779959976562 + 33733491857\pi \ , \\
c_0' &= 779959976562 - 33733491857\pi \ .
\end{aligned}$$

We now compute the chain of isogenous curves X_i's obtained via the Bost-Mestre AGM (note all computations are done to π^{20}):

$$\begin{aligned}
X_1 : y^2 = {} & 14509968966141x^6 + 13535473244274x^5 - 4366138213591x^4 - 383149059076x^3 \\
& + 4532268917237x^2 + 10611945668949x + 11501225120914
\end{aligned}$$

with roots

$$\begin{aligned}
a_1 &= 29969023457189 \ , \quad a_1' = 36816510168425 \ , \\
b_1 &= 2703407962350 \ , \quad b_1' = 41130794360331 \ , \\
c_1 &= 37949541236172 \ , \quad c_1' = 6221753140751 \ .
\end{aligned}$$

By our choice of the quadratic splitting it is immediately clear that these roots should lie over $\mathbb{Q}_{23}$ itself. For example, the discriminant of W_0 is given by

$$4Q_0(a_0)Q(b_0) = 4(a_0-c_0)(a_0-d_0)(b_0-c_0)(b_0-d_0) \ ,$$

from which all terms containing π vanishes and the remaining part is a square in $\mathbb{Q}_{23}$ because $X_0(23)$ is totally split. We already know that all the curves X_i's are totally split of Type B and their roots lie in the same p-adic discs as X_0; indeed one checks that

$$a_1 \equiv a_1' \mod \pi^2 \ , \quad b_1 \equiv b_1' \mod \pi^2 \quad \text{and} \quad c_1 \equiv c_1' \mod \pi^2 \ .$$

Here is the equation for X_2 and its roots:

$$X_2 : y^2 = 15963560922167x^6 + 8915045081136x^5 + 5655951820305x^4 + 7187214907216x^3 + 9290858991658x^2 + 18116669010963x - 9470171526445 ,$$

$$\begin{aligned} a_2 &= 15634233532478 , & a_2' &= 38514512500429 , \\ b_2 &= 41230679116716 , & b_2' &= 37806965241739 , \\ c_2 &= 18164834403771 , & c_2' &= 30030908259387 , \end{aligned}$$

with

$$a_1 \equiv a_1' \mod \pi^4 , \quad b_1 \equiv b_1' \mod \pi^4 \quad \text{and} \quad c_1 \equiv c_1' \mod \pi^4 .$$

And finally the equation for X_3 and its roots:

$$X_3 : y^2 = 13413380228472x^6 + 9889873468227x^5 + 11869333871359x^4 + 19069176773695x^3 - 9637185255233x^2 + 2318445679270x - 6104023778492 ,$$

$$\begin{aligned} a_3 &= 6361117409629 , & a_3' &= 6361117409629 , \\ b_3 &= 1577149810583 , & b_3' &= 36895404172314 , \\ c_3 &= 23050359306739 , & c_3' &= 15552288918781 . \end{aligned}$$

with

$$a_1 \equiv a_1' \mod \pi^8 , \quad b_1 \equiv b_1' \mod \pi^8 \quad \text{and} \quad c_1 \equiv c_1' \mod \pi^8 .$$

On the chain of Jacobians we wish to compute the kernel of g_0 and lift it. Note that we will switch between Mumford representations and actual divisors whenever suitable. First consider the diagram:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & J_n & \longrightarrow & \cdots & \xrightarrow{g_2} & J_2 & \xrightarrow{g_1} & J_1 & \xrightarrow{g_0} & J_0 \\ \cdots & \longrightarrow & \begin{matrix} Du_n \\ Dv_n \\ Dw_n \end{matrix} & \longrightarrow & \cdots & \longrightarrow & \begin{matrix} Du_2 \\ Dv_2 \\ Dw_2 \end{matrix} & \longrightarrow & \begin{matrix} Du_1 \\ Dv_1 \\ Dw_1 \end{matrix} & \longrightarrow & \mathcal{O} \end{array}$$

Since the Richelot isogeny is a 4-to-1 map, it is clear that Du_1, Dv_1 and Dw_1 (along with the zero divisor) form the kernel of g_0. But from the analysis on the isogeny we know that

$$\ker(g_0) = \left\{ \mathcal{O}, \left[(u_0, 0) - (u_0', 0)\right], \left[(v_0, 0) - (v_0', 0)\right], \left[(w_0, 0) - (w_0', 0)\right] \right\} \subseteq J_1 ,$$

which is isomorphic to V_4. In the Mumford representation, these are given by $\left[x^2 - sx + p, 0\right]$, where s is the sum of the two roots and p their product; since both are Weierstrass points,

the second component is simply 0. Hence we have

$$\begin{aligned} Du_1 &= \big[(u_0, 0) - (u_0', 0)\big] = \big[x^2 + 3772686830795x + 4779300317558, 0\big] \ , \\ Dv_1 &= \big[(v_0, 0) - (v_0', 0)\big] = \big[x^2 + 5235734615709x - 20478600731137, 0\big] \ , \\ Dw_1 &= \big[(w_0, 0) - (w_0', 0)\big] = \big[x^2 + 1906593082874x + 1490035220585, 0\big] \ . \end{aligned}$$

To lift these further onto J_2, we use the bisection method as previously described. That is, we wish to compute

$$Du_1 \longrightarrow \frac{1}{2}Du_1 \xrightarrow{\hat{g_1}} Du_2 \ .$$

We will not print the degree 16 polynomial here (i.e. the resultant of $S_1(k_0, k_1)$ and $S_0(k_0, k_1)$), which interested readers may find in last Appendix. These are its 16 roots for k_1 as computed by Magma:

$$\begin{aligned} k_1 &= \pm 19617456095355 \pm 35192479892568\pi \quad \text{or} \\ k_1 &= \pm 34557226984708 \pm 39185555306827\pi \quad \text{or} \\ k_1 &= \pm 36851057497971 \pm 33137217351539\pi \quad \text{or} \\ k_1 &= \pm 19478615780351 \pm 14888363433824\pi \ . \end{aligned}$$

This suggests some interesting structure for the polynomial itself, but we will not pursue it here. Note that the signs for k_1 do not matter – it simply causes k_0 to change signs which in turn causes a change of sign in the support of the bisection. This is neglected as it is mapped onto the next Jacobian. That is to say, all four k_1's map onto the same divisor on J_2. This agrees with our knowledge on the Richelot isogeny that it is a 4-to-1 map.

Taking, for example,

$$k_1 = 19617456095355 + 35192479892568\pi$$

yields

$$k_0 = 34676842943569 + 1907454218760\pi \ .$$

This gives the corresponding bisection as

$$\frac{1}{2}Du_1 = [P_1 + P_2] = [U(x), V(x)] \ ,$$

where

$$\begin{aligned}
U(x) &= x^2 + (3755966400993 + 4235709965178\pi)x + (2143338580354 + 5838461260230\pi) \ , \\
V(x) &= (964972109231 + 20754974766165\pi)x + (5538877812120 + 34312681664209\pi) \ , \\
P_1 &= (20843997281321 + 37869416972530\pi, 20700417432520 + 17537234561531\pi) \ , \\
P_2 &= (24338480333321 + 40747895489590\pi, 13552216979968 + 12473332310983\pi) \ .
\end{aligned}$$

Before mapping P_1 and P_2 to J_2, one first has to scale it by the square root of the x^6 coefficient of X_1 so that it lies on the curve $y^2 = P_1Q_1R_1$ (instead of $T_1y^2 = U_0V_0W_0$ as it currently does). Now mapping the scaled points via the dual Richelot isogeny, and then rescaling it back gives

$$\hat{g_1}(P_1) = \left[Q_1 + Q_1'\right] \ ,$$

where

$$\begin{aligned}
Q_1 &= (15588142880255 + 13614777038871\pi, 2026443975492 + 31565145522315\pi) \ , \\
Q_1' &= (3503913201810 + 37211337310263\pi, 1634554359251 + 10681002910033\pi) \ .
\end{aligned}$$

Similarly

$$\hat{g_1}(P_2) = \left[Q_2 + Q_2'\right] \ ,$$

where

$$\begin{aligned}
Q_2 &= (12952102174602 + 17872156829551\pi, 39129102600005 + 23905673565742\pi) \ , \\
Q_2' &= (34057150363331 + 36281579638141\pi, 36203107768550 + 25761328056179\pi) \ .
\end{aligned}$$

Combining everything we have lifted Du_1 to the divisor

$$\begin{aligned}
\hat{g_1}(Du_1) &= \left[Q_1 + Q_1' + Q_2 + Q_2'\right] \\
&= \left[x^2 + 36833651358680x + 5787826917764, 3303842326834x + 16005171221467\right] \ .
\end{aligned}$$

Note that there are four preimages of Du_1. Recall that while the Richelot isogeny doubles the periods of X_1, the map f_1 between the uniformisations $(K^\times)^2/H_2 \longrightarrow (K^\times)^2/H_1$ is given by the identity map. Therefore correspondingly we seek the preimage which is 'congruent' to Du_1 in the sense that the support of the two divisors are in the same p-adic discs. Because of the roundabout way we constructed g_i^{-1}, unfortunately we do not know for sure that such a divisor always exists. However, it certainly does in genus 1 and in view of our

numerical evidence, we are confident that this is always possible.

Theoretically the easiest way to obtain the other three preimages is to add the kernel of g_1 (which are again pairs of Weierstrass points) to the above divisor. But unfortunately this causes severe loss of precision inside Magma, so instead we will take four values of k_1, one from each quadruplets, and repeat the above process. Omitting the intermediate computations, here are the four preimages of Du_1:

$$\begin{aligned}
\left[x^2 + 36833651358680x + 5787826917764, 3303842326834x + 16005171221467\right] &, \\
\left[x^2 + 36833651358680x + 5787826917764, -3303842326834x - 16005171221467\right] &, \\
\left[x^2 + 570508136719x + 38814447073528, 39947032033123x + 23933496908852\right] &, \\
\left[x^2 + 570508136719x + 38814447073528, -39947032033123x - 23933496908852\right] &.
\end{aligned}$$

One immediately observes that these four preimages are in fact two pairs of opposite divisors. This is to be expected since the second component of Du_1 is the zero polynomial; hence the whole picture will be symmetric under reflection. Furthermore, it is worth noting that although we have passed through to $\mathbb{Q}_{23}(\pi)$ for the most part, the roots of the quadratics in these preimages are all $\mathbb{Q}_{23}$-rational, though this is not necessarily true in general. In this case the divisor we seek is either the third or the fourth one (which does not matter in the end), since the roots of the quadratic $x^2 + 570508136719x + 38814447073528$ are given by

$$\begin{aligned}
x = 16547544929867 &= 14 + 23 + 18 \times 23^2 + 5 \times 23^3 + 11 \times 23^4 + 14 \times 23^5 + \cdots , \\
x = 24308458147063 &= 21 + 2 \times 23 + 3 \times 23^2 + 22 \times 23^4 + 11 \times 23^5 + 9 \times 23^6 \cdots .
\end{aligned}$$

So we conclude that

$$Du_2 = \left[x^2 + 570508136719x + 38814447073528, 39947032033123x + 23933496908852\right] .$$

And similarly, the lifts of Dv_1 and Dw_1 are given by

$$\begin{aligned}
Dv_2 &= \left[x^2 + 28747176982521x + 15742432005809, 23856327829181x + 21330178054941\right] , \\
Dw_2 &= \left[x^2 + 14257352574105x + 16172605252402, 41179889101919x + 9512547229701\right] .
\end{aligned}$$

Codes for all of the above can be found in Appendix C. We can, in principle, go further and lift them to J_3, but technology (or our lack of proficiency with it) seems to be a limiting

factor, as we will discuss in the closing remarks. Nonetheless, lifting to J_2 should yield the periods accurate to π^8, which is already further than it is done in [Tei88].

4.10 Conclusion and Future Work

Once again recall the following

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & (K^\times)^2/H_n & \longrightarrow & \cdots & \xrightarrow{f_1} & (K^\times)^2/H_1 & \xrightarrow{f_0} & (K^\times)^2/H_0 \\
 & & \phi_n \downarrow \wr & & & & \phi_1 \downarrow \wr & & \phi_0 \downarrow \wr \\
\cdots & \longrightarrow & J_n & \longrightarrow & \cdots & \xrightarrow{g_1} & J_1 & \xrightarrow{g_0} & J_0 \\
 & & \uparrow & & & & \uparrow & & \uparrow \\
 & & X_n & & & & X_1 & & X_0
\end{array}$$

The bottom two rows are now well understood and we have seen, through an explicit example, how everything fits together in practice. The last remaining piece of the puzzle is the vertical maps ϕ_i's, which we will not cover in this thesis. Nonetheless, we can provide some degree of speculation on how this map could be obtained (hopefully most of these speculations will be proven in due time!).

We first return to genus 1, where the map between an elliptic curve and its Tate curve is given explicitly in [Sil94] (or see Section 3.3). It is essentially derived from the Weierstrass $\wp$-function and one can attempt to interpret this in terms of theta functions. Consider the odd theta function

$$\theta_{1,1}(z,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i(n+\frac{1}{2})^2\tau + 2\pi i(n+\frac{1}{2})(z+\frac{1}{2})} \ .$$

Letting $p = e^{\pi i\tau}$ (or $\tau = \dfrac{1}{\pi i}\log p$) and $w = e^{2\pi iz}$, this becomes

$$\begin{aligned}
\theta_{1,1}(z,\tau) &= \sum_{n\in\mathbb{Z}} e^{\pi i(n+\frac{1}{2})^2\left(\frac{1}{\pi i}\log p\right) + 2\pi i(n+\frac{1}{2})(z+\frac{1}{2})} \\
&= ip^{\frac{1}{4}}w^{\frac{1}{2}} \sum_{n\in\mathbb{Z}} (-1)^n p^{n^2+n} w^n \\
&= -ip^{\frac{1}{4}}w^{-\frac{1}{2}} \sum_{j\in\mathbb{Z}} (-1)^j p^{j^2-j} w^j \\
&= -ip^{\frac{1}{4}}w^{-\frac{1}{2}}\theta_T(p,w) \ ,
\end{aligned}$$

where we have relabelled $j = n+1$. Note that the summation $\theta_T(p,w)$ is precisely the

theta function given by Tate in [Tat97]. One useful property is the existence of a product formula for the sum. More precisely, the Jacobi triple product gives, for $q = p^2$,

$$\sum_{j\in\mathbb{Z}}(-1)^j q^{\frac{j^2-j}{2}} w^j = (1-w)\prod_{n=1}^{\infty}\left[(1-q^n)(1-q^n w)(1-q^n w^{-1})\right] \ .$$

The Weierstrass σ-function associated to a lattice $\Lambda \subseteq \mathbb{C}^2$ is defined by

$$\sigma(z,\Lambda) = e^{\frac{1}{2}(\frac{z}{w})^2+\frac{z}{w}} z \prod_{w\in\Lambda\setminus 0}\left(1-\frac{z}{w}\right) \ ,$$

which is related to $\wp(z)$ by

$$\wp(z) = -\frac{d^2}{dz^2}\log\sigma(z) \ .$$

If Λ is generated by 1 and τ, then one can show that the σ-function has the product expansion

$$\sigma(z,\tau) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta z^2-\pi i z}(1-w)\prod_{n\geq 1}\frac{(1-q^n w)(1-q^n w^{-1})}{(1-q^n)^2} \ ,$$

where η is the quasi-period associated to the period $1 \in \Lambda$. Note that the product is simply a normalised form of the product expansion of $\theta_T(p,w)$. Combining these, one can prove the classical relations which the Weierstrass $\wp$-function and its derivative satisfy and the map from $\overline{K}^*/q^{\mathbb{Z}}$ to the Tate curve. Furthermore, considering ϕ_n as n tends to infinity, the periods q^{2^n} tend to 0. In the limit we have $\theta_T(0,w) = 1-w$, since the only terms of $\theta_T(p,w)$ which do not vanish is when $i = 0$ and $i = 1$ (of course this can also be directly derived from the product expansion of $\sigma(z,\tau)$). This implies that

$$\begin{aligned}\wp(z) &= c - \frac{d^2}{dz^2}\left(\log(1-e^{2\pi i z})\right)\\ &= c - 4\pi^2\left(\frac{e^{-2\pi i z}}{(e^{-2\pi i z}-1)^2}\right)\\ &= c - 4\pi^2\frac{w}{(1-w)^2} \ .\end{aligned}$$

This last expression resembles that of the one used in Chapter 1.6 of [Sil94] (after some translation and rescaling). So this should provide insights into the overall strategy in genus 2. In genus 2, a fundamental theorem by Riemann states that there exists an odd theta function which has a zero of order one along the pull-back of the image of X in J of the Abel-Jacobi map to $\mathbb{C}$. This is explicitly computed in [Mum84] (using the standard choice

of sympletic basis), and for genus 2 this 'special' odd theta function 2 is given by

$$\theta \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} (z_1, z_2)(\Omega) \ .$$

Let $w_i = e^{2\pi i z_i}$ and we wish to evaluate the theta function at the matrix

$$\Omega = \frac{1}{\pi i} \begin{pmatrix} \log p_2 p_3 & -\log p_3 \\ -\log p_3 & \log p_1 p_3 \end{pmatrix} \ ,$$

which came from the linkage between complex and p-adic theta functions. This gives

$$\begin{aligned} \theta \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} (z_1, z_2)(\Omega) &= \sum_{(n_1,n_2)\in\mathbb{Z}^2} (p_2p_3)^{(n_1+\frac{1}{2})^2} (p_3)^{-(n_1+\frac{1}{2})(n_2+\frac{1}{2})} (p_1p_3)^{(n_2+\frac{1}{2})^2} w_1^{n_1+\frac{1}{2}} w_2^{n_2+\frac{1}{2}} (-1)^{n_2} (-i) \\ &= (-i)(w_1w_2)^{\frac{1}{2}} (p_1p_2)^{\frac{1}{4}} \sum_{(n_1,n_2)\in\mathbb{Z}^2} (-1)^{n_2} p_1^{n_2^2+n_2} p_2^{n_2^1+n_1} p_3^{(n_1-n_2)^2} w_1^{n_1} w_2^{n_2} \\ &= (-i)(w_1w_2)^{-\frac{1}{2}} (p_1p_2)^{\frac{1}{4}} \sum_{(i,j)\in\mathbb{Z}^2} (-1)^{j} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2} w_1^{i} w_2^{j} \ , \\ &= (-i)(w_1w_2)^{-\frac{1}{2}} (p_1p_2)^{\frac{1}{4}} \theta_T(p_1, p_2, p_3, w_1, w_2), \end{aligned}$$

where $i = n_1 + 1$ and $j = n_2 + 1$. Note the similarly between this summation and Tate's theta function in genus 1. Now we can define the sigma function as before

$$\sigma(z_1, z_2) = e^{-\frac{1}{2}(z_1\ z_2)A(z_1\ z_2)^{\mathrm{T}}} \theta \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} (z_1, z_2)(\Omega) \ ,$$

where A is a matrix of quasi-periods (see [Gra88]). The Weierstrass $\wp$-functions are now second partial derivatives of the sigma function

$$\wp_{ij} = -\frac{\partial^2}{\partial z_i \partial z_j} \log \sigma(z_1, z_2) \ .$$

Suppose we have $(z_1, z_2) = \phi\left((x_1, y_1), (x_2, y_2)\right)$, where ϕ is the Abel-Jacobi map from $J(X)$ to $(K^\times)^2/H_\Gamma$. Then Grant's paper [Gra88] gives formulae (due to Baker) that link $\wp_{ij}(z_1, z_2)$ to x_1, x_2, y_1 and y_2, for example the simplest of them being

$$\begin{aligned} \wp_{1,2} &= -\frac{1}{4} x_1 x_2 \ , \\ \wp_{2,2} &= \frac{1}{4}(x_1 + x_2) \ . \end{aligned}$$

We should also note that all these formulae require the model of the curve to be quintic, so work has to be done to apply them in our situation. In particular, we should pull back the divisor along the Richelot isogeny as far as we need, and then make a change of coordinates to a Rosenhain model.

Let us examine what happens as we apply the AGM to the curve. By lifting the divisor in $J(X)$, we will hopefully have 2 points, whose x-coordinates are the x_1 and x_2 we need. Furthermore, the theta function tends to $1 - w_1 w_2$ as n tends to infinity, so that the periods p_i tend to 0. Therefore if one is able to discern formulae for the vertical maps, even if only in the degenerate case, it seems plausible that one can compute the values of the required $\wp_{ij}$ and hence allowing us to pull-back the vertical map.

There is also work to be done on the computational aspect of things. Due to Magma's weakness in symbolic manipulations, parts of the computation on $X_0(23)$ had to be done with another software such as Pari, Maple or Sage. On the other hand, none of these softwares are as capable in solving equations over $\mathbb{Q}_{23}(\pi)$ as Magma. As a result we were forced to compromise in using both – which means that we do not have a complete function, as in the AGM over $\mathbb{C}$, that takes a curve and outputs the lifts of the zero divisor. Finally, precision seems to be an issue if one were to further lift the divisors to J_3. Although we have printed all results to π^{20}, we had to set the precision of $\mathbb{Q}_{23}(\pi)$ to π^{40} for Magma to work, and the roots of X_3 are too close together; we would have had to increase the precision a lot further for Magma to recognise it as a hyperelliptic curve. So after all the theoretical grounds are laid, there is certainly work to be done on improving this algorithm in practice.

Appendix A

Computing Periods for Genus 2 Curves over $\mathbb{C}$ (Magma)

The following code computes the period matrices (both the full and the Riemann form) of a complex genus 2 hyperelliptic curve in Magma (a similar programme was also written for Maple). We note that both Magma and Maple take different approaches in computing period integrals and experiementation shows that this runs faster than both programs (especially to high precision).

```
CC<i> := ComplexField(30);
RR := RealField(30);
II := Integers();
P<x> := PolynomialRing(CC);
Pi := Pi(RealField(30));
acc := II!20;


rightchoice := function(u1,u2,v1,v2,w1,w2)
/*
    Compute the right choice for AGM (Step 2 onwards).
    Takes all 8 possible choices and computes the minimum distance.
*/
    M := Matrix(P,8,3,[]);
    d := Matrix(RR,8,1,[]);
    c := 1;
    M[1,1]:=(x-v1)*(x-w1); M[1,2]:=(x-w2)*(x-u1); M[1,3]:=(x-u2)*(x-v2);
    M[2,1]:=(x-v1)*(x-w1); M[2,2]:=(x-w2)*(x-u2); M[2,3]:=(x-u1)*(x-v2);
    M[3,1]:=(x-v1)*(x-w2); M[3,2]:=(x-w1)*(x-u1); M[3,3]:=(x-u2)*(x-v2);
    M[4,1]:=(x-v1)*(x-w2); M[4,2]:=(x-w1)*(x-u2); M[4,3]:=(x-u1)*(x-v2);
```

```
    M[5,1]:=(x-v2)*(x-w1); M[5,2]:=(x-w2)*(x-u1); M[5,3]:=(x-u2)*(x-v1);
    M[6,1]:=(x-v2)*(x-w1); M[6,2]:=(x-w2)*(x-u2); M[6,3]:=(x-u1)*(x-v1);
    M[7,1]:=(x-v2)*(x-w2); M[7,2]:=(x-w1)*(x-u1); M[7,3]:=(x-u2)*(x-v1);
    M[8,1]:=(x-v2)*(x-w2); M[8,2]:=(x-w1)*(x-u2); M[8,3]:=(x-u1)*(x-v1);
    for i in [1..8] do
        d[i,1]:=&+[Abs(Roots(M[i][j])[1][1]-Roots(M[i][j])[2][1]):j in{1..3}];
        if d[i,1] lt d[c,1] then
            c := i;
        end if;
    end for;
    return M[c,1],M[c,2],M[c,3];
end function;


AGM := function(a,b,c,d,e,f);
/*
    Takes 6 complex numbers and computes their arithmetic-geometric mean
    according to Bost-Mestre's algorithm. Requires the 'rightchoice' function.
    It iterates until the desired precision and then iterates once more for
    safety measure. This implements Algorithm 2.16.
*/
    coeff := [a,b,c,d,e,f];
    T := CC!1;
    P := (x-coeff[1])*(x-coeff[2]);
    Q := (x-coeff[3])*(x-coeff[4]);
    R := (x-coeff[5])*(x-coeff[6]);
    err := 1;
    ex := 0;
while Abs(err) ge 10^(-acc/2) or ex le 2 do
    U := Derivative(Q)*R-Q*Derivative(R);
    V := Derivative(R)*P-R*Derivative(P);
    W := Derivative(P)*Q-P*Derivative(Q);
    M := Matrix(CC,3,3,
       [1,Coefficients(P)[2],Coefficients(P)[1],
        1,Coefficients(Q)[2],Coefficients(Q)[1],
        1,Coefficients(R)[2],Coefficients(R)[1]]);
    Delta := Determinant(M);
    t := 2*Sqrt(-Delta/Coefficients(U*V*W)[7]);
    T := T*t;
    u := [Roots(U)[1][1], Roots(U)[2][1]];
    v := [Roots(V)[1][1], Roots(V)[2][1]];
    w := [Roots(W)[1][1], Roots(W)[2][1]];
    P, Q, R, err := rightchoice(u[1],u[2],v[1],v[2],w[1],w[2]);
    if Abs(err) le 10^(-acc/2) then ex := ex+1; end if;
end while;
```

```
    z:=Sort([[Re(u[1]),Im(u[1])],[Re(u[2]),Im(u[2])],[Re(v[1]),Im(v[1])],
             [Re(v[2]),Im(v[2])],[Re(w[1]),Im(w[1])],[Re(w[2]),Im(w[2])]]);
    return z[1,1]+z[1,2]*i,z[3,1]+z[3,2]*i,z[5,1]+z[5,2]*i,T;
end function;
```

```
PeriodMatrix := function(a,b,c,d,e,f)
/*
    Take 6 distinct complex numbers (a,b,c,d,e,f) and returns the period matrix
    of the hyperelliptic curve defined by $y^2=(x-a)(x-b)(x-c)(x-d)(x-e)(x-f)$.
    This implements Algorithm 2.18.
*/
    coeff := [a,b,c,d,e,f];
    M := Matrix(CC,2,6,[]);
    bpoint := Sort([[Re(coeff[i]),i]:i in {1..6}])[1];
    mindis := 0.4*Min([Abs(coeff[i]-coeff[II!bpoint[2]]):
                       i in {1..6} diff {II!bpoint[2]}]);
    for i in [1..6] do
        M[1][i] := Arg(coeff[i]-coeff[II!bpoint[2]]+mindis);
        M[2][i] := Abs(coeff[i]-coeff[II!bpoint[2]]+mindis);
    end for;
    sorted:=Sort([[RR!M[1][i],RR!M[2][i],i]:i in {1..6}]);
/*
    This arranges the six initial roots by choosing the left-most point as
    its basepoint. The roots are then arranged first by argument with
    respect to the basepoint, then by distance. This method is taken
    from Maple.
*/
    coeff := [coeff[II!sorted[i,3]]:i in {1..6}];
    AGM1,AGM2,AGM3,T := AGM(coeff[1],coeff[2],coeff[3],coeff[4],coeff[5],coeff[6]);
    A := Matrix(CC,3,2,[
        Pi*T*i/((AGM2-AGM1)*(AGM3-AGM1)),
        Pi*T*AGM1*i/((AGM2-AGM1)*(AGM3-AGM1)),
        Pi*T*i/((AGM2-AGM1)*(AGM3-AGM2)),
        Pi*T*AGM2*i/((AGM2-AGM1)*(AGM3-AGM2)),
        Pi*T*i/((AGM3-AGM2)*(AGM3-AGM1)),
        Pi*T*AGM3*i/((AGM3-AGM1)*(AGM3-AGM2))]);
    S := [[1,1,1],[1,-1,1],[1,1,-1],[1,-1,-1]];
    n:=II!Sort([[Abs(&+[S[i,j]*A[j,1] : j in [1..3]]),i] : i in[1..4]])[1][2];
    A := Matrix(CC,3,2,[
        S[n,1]*A[1,1],S[n,1]*A[1,2],
        S[n,2]*A[2,1],S[n,2]*A[2,2],
        S[n,3]*A[3,1],S[n,3]*A[3,2]]);
/*  Fixes the sign of the periods such that $A[1,i]-A[2,i]+A[3,i]=0$  */
    AGM1,AGM2,AGM3,T := AGM(coeff[1],coeff[6],coeff[2],coeff[3],coeff[4],coeff[5]);
    B := Matrix(CC,3,2,[
        Pi*T*i/((AGM2-AGM1)*(AGM3-AGM1)),
        Pi*T*AGM1*i/((AGM2-AGM1)*(AGM3-AGM1)),
        Pi*T*i/((AGM2-AGM1)*(AGM3-AGM2)),
        Pi*T*AGM2*i/((AGM2-AGM1)*(AGM3-AGM2)),
```

```
        Pi*T*i/((AGM3-AGM2)*(AGM3-AGM1)),
        Pi*T*AGM3*i/((AGM3-AGM1)*(AGM3-AGM2))]);
/*  Computes the Type B-periods  */
    S := [[1,2],[1,3],[2,1],[2,3],[3,1],[3,2]];
    match := 0;
    for i in S do
        for j,k in [1..3] do
            for n in [[-1,-1],[-1,1],[1,-1],[1,1]] do
                C1 := Matrix(CC,2,2,[A[i[1],1],A[i[2],1],
                                     A[i[1],2],A[i[2],2]]);
                C2 := Matrix(CC,2,2,[
                n[1]*B[j,1]+n[2]*B[k,1], n[2]*B[k,1],
                n[1]*B[j,2]+n[2]*B[k,2], n[2]*B[k,2]]);
                C := C1^-1*C2;
                CIm := Matrix(CC,2,2,[Im(C[1,1]),Im(C[1,2]),
                                      Im(C[2,1]),Im(C[2,2])]);
                evalues := [i[1]: i in Eigenvalues(CIm)];
                if Abs(C[1,2]-C[2,1]) lt 10^-acc
                and RR!evalues[1] gt 10^-acc
                and RR!evalues[2] gt 10^-acc then
                bigperiodmatrix := Matrix(CC,2,4,[
                    C1[1][1],C1[1][2],C2[1][1],C2[1][2],
                    C1[2][1],C1[2][2],C2[2][1],C2[2][2]]);
                smallperiodmatrix := C;
                match := 1;
                break;
                end if;
            end for;
        if match eq 1 then break; end if;
        end for;
    if match eq 1 then break; end if;
    end for;
/*  By trial and error find the values in $B$ such that the resulting matrix is
    Riemann  */
    return bigperiodmatrix, smallperiodmatrix;
end function;
```

Appendix B

Computing Tiny Coleman Integrals for Genus 1 Curves over $\mathbb{Q}_p$ (SAGE)

This takes an elliptic curve with split multiplicative reduction E, two points $P, Q \in E$ which lie in the same residue disc, and computes the tiny Coleman integration between the two points. It is quadratically convergent, whereas the existing one in Sage is linear. This implements Algorithm 3.11.

```
def p_adic_landen(self,P,Q):
#   Takes a elliptic cuve E and two points $P,Q$ on $E$ in the same disc
#   and returns the constant $u$ (which depends only on $E$) and the preimages
#   of $P$ & $Q$ on the Tate curve $E_q$, $phi_p$ & $phi_q$. The (tiny) Coleman
#   integral from $P$ to $Q$ is then given by $u*(log(phi_q/phi_p))$.
#   This implements Algorithm 3.11.
    prec = self.base().precision_cap()
    a2 = self.hyperelliptic_polynomials()[0].list()[2]
    E1 = K(self.weierstrass_points()[1][0].residue(prec-1).lift())
    E2 = K(self.weierstrass_points()[2][0].residue(prec-1).lift())
    E3 = K(self.weierstrass_points()[3][0].residue(prec-1).lift())
    if ((E2-E1)/(E3-E1)).residue(1)==1:
        e1,e2,e3 = E1,E2,E3
    elif ((E1-E2)/(E3-E2)).residue(1)==1:
        e1,e2,e3 = E2,E1,E3
    elif ((E1-E3)/(E2-E3)).residue(1)==1:
        e1,e2,e3 = E3,E1,E2
    else:
```

```
        raise ValueError, "E does not have split multiplicative reduction."
#   Checks that $E$ has split multiplicative reduction.
    x_p0, y_p0 = P[0], P[1]
    x_q0, y_q0 = Q[0], Q[1]
    A0 = e2-e1
    B0 = e3-e1
    B1 = B0*((A0/B0).sqrt())
    A1 = (A0+B0+2*B1)/4
    x_p1 = (x_p0+(e1+a2)/2)*(1+(1-4*A1*(A1-B1)/(x_p0+(e1+a2)/2)^2).sqrt())/2
    y_p1 = y_p0*(1-(A1*(A1-B1))/x_p1^2)^-1
    x_q1 = (x_q0+(e1+a2)/2)*(1+(1-4*A1*(A1-B1)/(x_q0+(e1+a2)/2)^2).sqrt())/2
    y_q1 = y_q0*(1-(A1*(A1-B1))/x_q1^2)^-1
    while (A1-B1).valuation() < prec:
        B2 = B1*(A1/B1).sqrt()
        A2 = (A1+B1+2*B2)/4
        x_p2 = x_p1*((1+K(1+(A1-B1)/x_p1).sqrt())/2)^2
        y_p2 = y_p1*(1-(A1-B1)^2/(16*x_p2^2))^-1
        x_q2 = x_q1*((1+K(1+(A1-B1)/x_q1).sqrt())/2)^2
        y_q2 = y_q1*(1-(A1-B1)^2/(16*x_q2^2))^-1
        A1, B1 = A2, B2
        x_p1, y_p1 = x_p2, y_p2
        x_q1, y_q1 = x_q2, y_q2
    u = (1/(4*B1)).sqrt()
    phi_p = (2*u*y_p2-x_p2)/(2*u*y_p2+x_p2)
    phi_q = (2*u*y_q2-x_q2)/(2*u*y_q2+x_q2)
    return u,phi_p,phi_q
```

Appendix C

Lifting the Richelot Isogeny for Genus 2 Curves over $\mathbb{Q}_p$ [1] (Magma)

The following codes takes a divisor on a genus 2 curve X_0 over $\mathbb{Q}_p$ and lifts it along a chain of Richelot isogenies using Magma. Note that it is, as it stands now, not a program in that one has to manually change parts of the code for it to function (it is currently taking $X_0 = X_0(23)$ and lifting the divisor $[u1 + u2]$, the kernel of g_0 in X_1). Furthermore, as Magma is not specialised in symbolic manipulations, a portion of this code has to be run on Pari (or Maple); details of the Pari code used is in the last Appendix.

```
K := pAdicRing(23, 20);
L<x> := PolynomialRing(K); L<pi> := TotallyRamifiedExtension(K,x^2+23);
LL<x> := PolynomialRing(L);

//First Iteration (F=X_0=X_0(23) here)
F := x^6-14*x^5+57*x^4-106*x^3+90*x^2-16*x-19;
a := -11525234105850519623491923+14969170352692467402990 29*pi;
b := -11525234105850519623491923-14969170352692467402990 29*pi;
c := 23050468211701039246983857;
d := 8639268500624383842178795;
e := 59260413317041349257417850 0+16549949299669492206678 34*pi;
f := 59260413317041349257417850 0-16549949299669492206678 34*pi;
T := (a*b*(e+f-c-d)-c*d*(e+f-a-b)+e*f*(c+d-a-b))/((c+d-a-b)*(e+f-a-b)*(e+f-c-d));
P := (x-a)*(x-b);Q := (x-c)*(x-d);R := (x-e)*(x-f);
U := Derivative(Q)*R-Q*Derivative(R);
V := Derivative(R)*P-R*Derivative(P);
```

```
W := Derivative(P)*Q-P*Derivative(Q);
u1 := Roots(U)[1][1]; u2 := Roots(U)[2][1];
v1 := Roots(V)[1][1]; v2 := Roots(V)[2][1];
w1 := Roots(W)[1][1]; w2 := Roots(W)[2][1];
FF := (x-u1)*(x-u2)*(x-v1)*(x-v2)*(x-w1)*(x-w2)/T;
//Second Iteration (FF=X_1, FFF=X_2)
a:=v2; b:=w1; c:=u2; d:=w2; e:=u1; f:=v1;
T := T*(a*b*(e+f-c-d)-c*d*(e+f-a-b)+e*f*(c+d-a-b))/((c+d-a-b)*(e+f-a-b)*(e+f-c-d));
P := (x-a)*(x-b);Q := (x-c)*(x-d);R := (x-e)*(x-f);
U := Derivative(Q)*R-Q*Derivative(R);
V := Derivative(R)*P-R*Derivative(P);
W := Derivative(P)*Q-P*Derivative(Q);
u1 := Roots(U)[1][1]; u2 := Roots(U)[2][1];
v1 := Roots(V)[1][1]; v2 := Roots(V)[2][1];
w1 := Roots(W)[1][1]; w2 := Roots(W)[2][1];
FFF := (x-u1)*(x-u2)*(x-v1)*(x-v2)*(x-w1)*(x-w2)/T;


Richelot := function(P)
/*
    Richelot isogeny, takes a point $P$ on $FF$ and returns two points on $FFF$.
    Note that technically both the input and output are points of the monic
    version of $FF$ and $FFF$ respectively, so one would have to scale the
    points before and after.
*/
    if P[2] eq 0 then
        P[2] := 1;
    end if;
/*
    If $P[2]=0$ then it is a Weierstrass point and maps to another Weierstrass
    point. Hence it is safe to set $P[2]=0$ to avoid compute 0/0.
*/
    phi_0 := (P[1]-a)*(P[1]-b)*(c+d-e-f)+(P[1]-c)*(P[1]-d)*(e+f-a-b);
    phi_1 := -(P[1]-a)*(P[1]-b)*(c+d-e-f)*(u1+u2)-(P[1]-c)*(P[1]-d)*(e+f-a-b)*(v1+v2);
    phi_2 := (P[1]-a)*(P[1]-b)*(c+d-e-f)*u1*u2+(P[1]-c)*(P[1]-d)*(e+f-a-b)*v1*v2;
    z1_x := (-phi_1-Sqrt(L!(phi_1^2-4*phi_0*phi_2)))/(2*phi_0);
    z1_y := (P[1]-a)*(P[1]-b)*(c+d-e-f)*(z1_x-u1)*(z1_x-u2)*(P[1]-z1_x)/P[2];
    z2_x := (-phi_1+Sqrt(L!(phi_1^2-4*phi_0*phi_2)))/(2*phi_0);
    z2_y := (P[1]-a)*(P[1]-b)*(c+d-e-f)*(z2_x-u1)*(z2_x-u2)*(P[1]-z2_x)/P[2];
    return [z1_x,z1_y],[z2_x,z2_y];
end function;


DualRichelot := function(Q)
/*
```

```
    The dual isogeny, takes a point $Q$ in $FFF$ and returns two points on
    $FF$. Once again the points have to be rescaled before and after. This
    is not actually used below, but is included for completeness.
*/
    if Q[2] eq 0 then
        Q[2] := 1;
    end if;
    phi_0 := ((Q[1]-u1)*(Q[1]-u2)*(c+d-e-f)+(Q[1]-v1)*(Q[1]-v2)*(e+f-a-b));
    phi_1 := (-(Q[1]-u1)*(Q[1]-u2)*(c+d-e-f)*(a+b)-(Q[1]-v1)*(Q[1]-v2)*(e+f-a-b)*(c+d));
    phi_2 := ((Q[1]-u1)*(Q[1]-u2)*(c+d-e-f)*a*b+(Q[1]-v1)*(Q[1]-v2)*(e+f-a-b)*c*d);
    z1_x := (-phi_1-Sqrt(L!(phi_1^2-4*phi_0*phi_2)))/(2*phi_0);
    z1_y := (z1_x-a)*(z1_x-b)*(c+d-e-f)*(Q[1]-u1)*(Q[1]-u2)*(z1_x-Q[1])/(Q[2]);
    z2_x := (-phi_1+Sqrt(L!(phi_1^2-4*phi_0*phi_2)))/(2*phi_0);
    z2_y := (z2_x-a)*(z2_x-b)*(c+d-e-f)*(Q[1]-u1)*(Q[1]-u2)*(z2_x-Q[1])/(Q[2]);
    return [z1_x,z1_y],[z2_x,z2_y];
end function;


//Bisecting Divisor
/*
    This takes the divisor ([u1+u2] on $FF$ in this case) and computes the
    preimage of the Richelot isogeny on $FFF$. Note that this part requires
    some help from Pari or Maple. The degree 16 polynomial first has to be
    computed in Pari/Maple before Magma can solve it over $Q_{23}(\pi)$.
    The roots (i.e. values of $k1$) are then put back into Pari/Maple to
    obtain the polynomials S1 and S0. Then Magma is able to compute the rest.
*/
for i := 1 to 16 do
Roots(16218451949283098907098342 73*x^16+731601849150059361223515573*x^14+
      1008319309956928654460790 48*x^12+105861399100794220919257243 3*x^10+
      6590531480690362977211362 78*x^8+692678393089642218813023342*x^6+
      1227254938697977444679939316*x^4+41629178989467405923303370 0*x^2+
      4492293396595075830564630 37)[i,1];
end for;
S1 := #Input from Pari/Maple#
S0 := #Input from Pari/Maple#
if #Roots(Gcd(S1,S0)) eq 0 then print("Lower precision"); end if;
L!Roots(Gcd(S1,S0))[1][1];
k0:= -17941281554531385703*pi - 1642411916650948342733;
k1:= 71712383877152713128554590043 54*pi+24286784622717622225346255220993;

f6:=19560851328230517571389586 2395;
f5:=-42496218304875262690491620 0784;
f4:=40944765086454416842285796 7194;
f3:=-43478855146441628960287913 1169;
```

```
f2:=-42197641991410462563608473469 1;
f1:=-3339719479486363340142724469 73;
f0:=3615085967408873701329673168 21;
f:=f6*x^6+f5*x^5+f4*x^4+f3*x^3+f2*x^2+f1*x+f0;
a:=0;b:=0;
s:=-952285979047593664384812;
p:=-267879165965281691699340;
/*  f_i are coefficients of $FF$, $s$ and $p$ are sum and products
    of $u1$ and $u2$ */
g4:=f6-k1^2;
g3:=s*f6+f5+k1^2*s-2*k0*k1;
g2:=(s^2-p)*f6+s*f5+f4+2*k0*k1*s-k1^2*p+2*a*k1-k0^2;
g1:=(s^3-2*p*s)*f6+(s^2-p)*f5+s*f4+f3+k0^2*s-2*k0*k1*p+2*b*k1+2*a*k0;
g0:=(s^4-3*p*s^2+p^2)*f6+(s^3-2*p*s)*f5+(s^2-p)*f4+s*f3+f2-k0^2*p+2*b*k0-a^2;
g:=g4*x^4+g3*x^3+g2*x^2+g1*x+g0;
u11:=L!(g3/(2*g4));
u10:=L!(((g2/g4)-u11^2)/2);
x1 := Roots(x^2+u11*x+u10)[1,1];
x2 := Roots(x^2+u11*x+u10)[2,1];
C := HyperellipticCurve(FF);
J := Jacobian(C);
P1 := Points(C,29337386820674748021417612 2)[1];
P2 := Points(C,-69257250904158371450950379 3)[1];
P3 := Points(C,x1)[1];
P4 := Points(C,x2)[1];
D:=P3-(-P4);P1-P2;D+D;
/*
    $[P3+P4]$ is the bisection of $[P1+P2]$ ($=[u1+u2]$). One has to
    manually check the signs of the $y$- coordinate of $P3$ and $P4$ to
    make sure they are right.
*/


//Rescaling $P3$ & $P4$ so that the curve is monic
C := HyperellipticCurve(FFF);
J := Jacobian(C);
P3:=[L!P3[1],L!P3[2]];
P4:=[L!P4[1],L!P4[2]];
if Valuation(Evaluate(FF,P3[1])-P3[2]^2) le 20 then
    print("Error: Check P3");
elif Valuation(Evaluate(FF,P4[1])-P4[2]^2) le 20 then
    print("Error: Check P4"); end if;
P3[2]:=P3[2]/Sqrt(L!LeadingCoefficient(FF));
P4[2]:=P4[2]/Sqrt(L!LeadingCoefficient(FF));
if Valuation(Evaluate(FF/LeadingCoefficient(FF),P3[1])-P3[2]^2) le 20 then
```

```
    print("Error: Check P3");
elif Valuation(Evaluate(FF/LeadingCoefficient(FF),P4[1])-P4[2]^2) le 20 then
    print("Error: Check P4"); end if;


//Applying Richelot to P3
Q1,Q2:=Richelot(P3);
Q1:=[L!Q1[1],L!Q1[2]*Sqrt(L!LeadingCoefficient(FF))];
Q2:=[L!Q2[1],L!Q2[2]*Sqrt(L!LeadingCoefficient(FF))];
if Valuation(Evaluate(FFF,Q1[1])-Q1[2]^2) le 20 then
    print("Error: Check Q1");
elif Valuation(Evaluate(FFF,Q2[1])-Q2[2]^2) le 20 then
    print("Error: Check Q2"); end if;
if Valuation(Q1[2]-Points(C,Q1[1])[1][2]) gt 20 then
    Q1:=Points(C,Q1[1])[1];
elif Valuation(Q1[2]-Points(C,Q1[1])[2][2]) gt 20 then
    Q1:=Points(C,Q1[1])[2];end if;
if Valuation(Q2[2]-Points(C,Q2[1])[1][2]) gt 20 then
    Q2:=Points(C,Q2[1])[1];
elif Valuation(Q2[2]-Points(C,Q2[1])[2][2]) gt 20 then
    Q2:=Points(C,Q2[1])[2];end if;
D1:=Q1-(-Q2);


//Applying Richelot to P4
Q3,Q4:=Richelot(P4);
Q3:=[L!Q3[1],L!Q3[2]*Sqrt(L!LeadingCoefficient(FF))];
Q4:=[L!Q4[1],L!Q4[2]*Sqrt(L!LeadingCoefficient(FF))];
if Valuation(Evaluate(FFF,Q3[1])-Q3[2]^2) le 20 then
    print("Error: Check Q3");
elif Valuation(Evaluate(FFF,Q4[1])-Q4[2]^2) le 20 then
    print("Error: Check Q4"); end if;
if Valuation(Q3[2]-Points(C,Q3[1])[1][2]) gt 20 then
    Q3:=Points(C,Q3[1])[1];
elif Valuation(Q3[2]-Points(C,Q3[1])[2][2]) gt 20 then
    Q3:=Points(C,Q3[1])[2];end if;
if Valuation(Q4[2]-Points(C,Q4[1])[1][2]) gt 20 then
    Q4:=Points(C,Q4[1])[1];
elif Valuation(Q4[2]-Points(C,Q4[1])[2][2]) gt 20 then
    Q4:=Points(C,Q4[1])[2];end if;
D2:=Q3-(-Q4);


print("");
D:=D1+D2;
```

```
Ker1:=Points(C,u1)[1]-Points(C,u2)[1];
Ker2:=Points(C,v1)[1]-Points(C,v2)[1];
Ker3:=Points(C,w1)[1]-Points(C,w2)[1];

u1;u2;
Roots(D[1]);
Roots((D+Ker1)[1]);
Roots((D+Ker2)[1]);
Roots((D+Ker3)[1]);
/*
    This computes all four divisors by adding the kernel of the isogeny
    to the first obtained answer. As mentioned in the paper this causes
    severe loss of accuracy and therefore only the first divisor $D$
    should be taken. One should take a different value of $k1$ and redo
    the computation to obtain the other preimages.
*/
```

Appendix D

Lifting the Richelot Isogeny for Genus 2 Curves over $\mathbb{Q}_p$ [2] (Pari)

These Pari codes fill in the missing gap in the previous section.

```
f6=19560851328230517571389586 2395;
f5=-42496218304875262690491620 0784;
f4=40944765086454416842285796 7194;
f3=-43478855146441628960287913 1169;
f2=-42197641991410462563608473 4691;
f1=-33397194794863633401427244 6973;
f0=36150859674088737013296731 6821;
a=0; b=0;
s=-952285979047593664384812;
p=-26787916596528169169934 0;
g4=f6-k1^2;
g3=s*f6+f5+k1^2*s-2*k0*k1;
g2=(s^2-p)*f6+s*f5+f4+2*k0*k1*s-k1^2*p+2*a*k1-k0^2;
g1=(s^3-2*p*s)*f6+(s^2-p)*f5+s*f4+f3+k0^2*s-2*k0*k1*p+2*b*k1+2*a*k0;
g0=(s^4-3*p*s^2+p^2)*f6+(s^3-2*p*s)*f5+(s^2-p)*f4+s*f3+f2-k0^2*p+2*b*k0-a^2;
u11=g3/(2*g4); u10=((g2/g4)-u11^2)/2;
s11=(g1/g4)-2*u10*u11; s10=(g0/g4)-u10^2;
S11=8*s11*(k1^2-f6)^3; S10=64*s10*(k1^2-f6)^4;
pol=polresultant(S10,S11,k0);
pol=pol/(k1^2-f6)^8;pol=pol/2^16; pol;
subst(S11, k1, 71712383877152713128554590043 54*pi+24286784622717622225346255220993);
subst(%, k0, x)
subst(S10, k1, 71712383877152713128554590043 54*pi+24286784622717622225346255220993);
subst(%, k0, x)
/*  pol is the degree 16 polynomial, then S11 and S10 are the polynomials
    needed in Magma  */
```

Bibliography

[Bak97] H. Baker. *Abel's Theorem and the Allied Theory.* Cambridge University Press, 1897.

[Bal15] J. Balakrishnan. Explicit p-adic methods for elliptic and hyperelliptic curves,. *Advances on Superelliptic Curves and their Applications*, pages 260–284, 2015.

[BBK10] J. Balakrishnan, R. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. *Algorithmic Number Theory*, 6197:16–31, 2010.

[BGR84] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean Analysis: A Systematic Approach to Rigid Analytic Geometry.* Springer-Verlag New York Inc, 1984.

[BM88] J.-B. Bost and J.-F. Mestre. Moyenne arithméto-géométrique et périodes des courbes de genre 1 et 2. *Gazette des Mathématiciens*, 38:36–64, 1988.

[Bre76] R. Brent. Fast multiple-precision evaluation of elementary functions. *Journal of the Association for Computing Machinery*, 23:242–251, 1976.

[CF96] J. Cassels and E. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Cambridge University Press, 1996.

[Cox84] D. Cox. The arithmetic-geometric mean of Gauss. *L'Enseignement Mathematique*, 30:275–330, 1984.

[CS86] G. Cornell and J. Silverman. *Arithmetic Geometry.* Springer-Verlag New York Inc., 1986.

[CT13] J. Cremona and T. Thongjunthug. The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms. *Journal of Number Theory*, 133(8):2813–2841, 2013.

[DS00] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer-Verlag New York Inc., 2000.

[DvH99] B. Deconinck and M. van Hoeij. Computing Riemann matrices of algebraic curves. 1999.

[FK80] H. Farkas and I. Kra. *Riemann Surfaces*. Springer-Verlag New York Inc., 1980.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1:243–265, 2007.

[GM17] X. Guitart and M. Masdeu. Periods of modular GL_2-type abelian varieties and p-adic integration. *Published online 1st March 2017 (https://doi.org/10.1080/10586458.2017.1284624)*, 2017.

[Got59] E. Gottschling. Explizite Bestimmung der randflaechen des Fundamentalbereiches der Modulgruppe zweiten Grade. *Mathematische Annalen*, 138:103–124, 1959.

[Gra88] D. Grant. A generalisation of Jacobi's derivative formula to dimension two. *Journal für die reine und angewandte Mathematik*, 392:125–136, 1988.

[GvdP80] L. Gerritzen and van der Put. *Schottky Groups and Mumford Curves*. Springer-Verlag New York Inc, 1980.

[HM89] G. Henniart and J.-F. Mestre. Moyenne arithmético-géométrique p-adique. *Comptes Rendus de l'Académie des Sciences*, 308:391–395, 1989.

[Igu72] J. Igusa. *Theta Functions*. Springer-Verlag New York Inc., 1972.

[Jar08] F. Jarvis. Higher genus arithmetic-geometric means. *The Ramanujan Journal*, 17:1–17, 2008.

[Kad07] S. Kadziela. Rigid analytic uniformization of curves and the study of isogenies. *Acta Applicandae Mathematicae*, 99:185–204, 2007.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[Lei05] F. Leitenberger. About the group law for the Jacobi variety of a hyperelliptic curve. *Contributions to Algebra and Geometry*, 46:125–130, 2005.

[MD73] Y. Manin and V. Drinfeld. Periods of p-adic Schottky groups. *Journal für die reine und angewandte Mathematik*, 262/263:239–247, 1973.

[MPT15] J. Miret, J. Pujolàs, and N. Thériault. Bisection of genus 2 curves with a real model. *Bulletin of the Belgian Mathematical Society*, 22:589–602, 2015.

[Mum72] D. Mumford. An analytic construction of degenerating curves over complete local rings. *Compositio Mathematica*, 24:129–174, 1972.

[Mum74] D. Mumford. *Abelian Variety*. Oxford University Press, 1974.

[Mum83] D. Mumford. *Tata Lectures on Theta I*. Modern Birkhäuser Classics, 1983.

[Mum84] D. Mumford. *Tata Lectures on Theta II*. Modern Birkhäuser Classics, 1984.

[MWZ96] A. Menezes, Y. H. Wu, and R. Zuccherato. An elementary introduction to hyperelliptic curves. *Technical Report CORR 96-19, Department of C&O, University of Waterloo*, 1996.

[Ser59] J. Serre. *Groupes Algébriques et Corps de Classes*. Hermann, Paris, 1959.

[Sie64] C. Siegel. *Symplectic Geometry*. Academic Press, New York and London, 1964.

[Sil86] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag New York Inc., 1986.

[Sil94] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag New York Inc., 1994.

[Smi05] B. Smith. Explicit endomorphisms and correspondences. *PhD Thesis, University of Sydney*, 2005.

[SvS12] J. Spandaw and D. van Straten. Hyperelliptic integrals and generalised arithmeticgeometric mean. *The Ramanujan Journal*, 28:61–78, 2012.

[Tat97] J. Tate. A review of non-archimedean elliptic functions. In J. Coates and S. T. Yau, editors, *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, pages 310–332. International Press of Boston Inc, 1997.

[Tei88] J. Teitelbaum. p-adic periods of genus two Mumford-Schottky curves. *Journal für die reine und angewandte Mathematik*, 385:117–151, 1988.

[Tho70] C. Thomae. Beitrag zur Bestimmung von $\theta(0, 0, ...0)$ durch die Klassenmoduln algebraischer Funktionen. *Journal für die reine und angewandte Mathematik*, 71:201–222, 1870.

[Wam06] P. Wamelen. Computing with the analytic Jacobian of a genus 2 curve. In *Discovering mathematics with Magma*, pages 117–135. Springer-Verlag Berlin, 2006.