UNIVERSITY OF CALIFORNIA

Los Angeles

Generalized Atkin Polynomials and Non-Ordinary Hyperelliptic Curves

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Mathematics

by

Matthew Ernest Lane

2012

ABSTRACT OF THE DISSERTATION

Generalized Atkin Polynomials and Non-Ordinary

Hyperelliptic Curves

by

Matthew Ernest Lane

Doctor of Philosophy in Mathematics

University of California, Los Angeles, 2012

Professor William Duke, Chair

There exists a sequence of orthogonal polynomials with many interesting properties from the standpoint of number theory. These polynomials are called Atkin polynomials, and they can be constructed using the theory of modular forms for the group $PSL_2(\mathbb{Z})$. Closed formulas for these polynomials are known, and their zeros provide information about supersingular elliptic curves.

In this dissertation, we construct an infinite collection of sets of orthogonal polynomials, of which the Atkin polynomials are but one example. These polynomials are constructed using the theory of modular forms for the Hecke triangle groups G_m, as well as the theory of hypergeometric functions. As in the previously known case, the zeros of this larger family of polynomials provide information about curves. In this setting, however, the curves are hyperelliptic, and the zeros detect whether or not certain curves are ordinary. We show how these curves arise and give proofs generalizing the known properties of the Atkin polynomials. We also interpret these generalized Atkin polynomials within the framework of period functions and weakly holomorphic modular forms, and prove some new results on the Fourier coefficients of certain modular integrals.

The dissertation of Matthew Ernest Lane is approved.

Chandrashekhar Khare

Don Blasius

Christian Fronsdal

William Duke, Committee Chair

University of California, Los Angeles

2012

to Meg

Contents

List of Figures

List of Tables

Acknowledgements

I would like to thank a number of people who have helped me during the course of my graduate study. My advisor, Bill Duke, was a tremendous resource in guiding me down the path that lead to the problem discussed in this thesis. He also exposed me to a lot of great mathematics along the way. I am grateful for the time he has spent to increase the scope and the depth of my mathematical knowledge.

Thanks also to Don Blasius, Chandrashekhar Khare, and Rizwan Khan for the number theory courses and seminars I was fortunate enough to attend. I learned a great deal from the courses they offered, and I appreciate the support they have provided both inside and outside of the classroom.

I would also like to thank my peers in the mathematics department for many insightful conversations over the years, both mathematical and otherwise. Special thanks to Patrick Allen, Tom Goldstein, Eamonn Tweedy, Jack Buttcane, Sungjin Kim, Yingkun Li, and my officemate Jacques Benatar. Thanks also to the many friends outside of the mathematics department for their support over the past several years.

I owe a tremendous amount to my parents and grandmother for always encouraging me to pursue my education, and for providing all manner of support throughout my academic career. Thank you for all your help through the years.

Finally, my wife Meg has been an exceptional source of emotional support throughout my years of graduate study. Thank you for sharing in the highs and helping me through the lows. Without your support, my sanity and my waistline would surely have suffered.

Vita

Matthew Ernest Lane graduated from Princeton University in 2005 with a bachelor's degree in mathematics. After working for a year in San Francisco, he enrolled in graduate school at the University of California, Los Angeles in the fall of 2006. He received his master's degree in mathematics in 2007. In 2010 he received the Sorgenfrey Distinguished Teaching Award in recognition of valuable teaching contributions to the Mathematics department. Some of his work in popular mathematics has been published in *The National Association for Media Literacy Education's Journal of Media Literacy Education*, and in the book *Mathematics in Popular Culture.*

CHAPTER 1

Introduction

In the late 1980's, A.O.L. Atkin discovered a remarkable sequence of monic orthogonal polynomials whose zeros provide information about elliptic curves. To construct these polynomials, let $\Gamma = PSL_2(\mathbb{Z})$ denote the usual modular group generated by the elements

$$\begin{aligned} S &= \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \\ T &= \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

and let E_4 and E_6 denote the weight 4 and weight 6 Eisenstein series for Γ (see Chapter 2 for precise definitions of these objects). Define the functions $\Delta(\tau)$ and $j(\tau)$ via the equations

$$\begin{aligned} \Delta(\tau) &= \frac{1}{1728}\left(E_4^3(\tau) - E_6^2(\tau)\right), \\ j(\tau) &= \frac{E_4^3(\tau)}{\Delta(\tau)}. \end{aligned}$$

It is well known that j is holomorphic on the upper half plane $\mathbb{H} = \{\tau = x + iy : y > 0\}$, and has a simple pole at $i\infty$. This latter fact is easily seen from the q-expansion of j; if we set $q = e^{2\pi i\tau}$, then we have

$$j(\tau) = \sum_{n=-1}^{\infty} a(n)q^n,$$

where, remarkably, the coefficients $a(n)$ are always integers (the first few are given by $a(-1) = 1$, $a(0) = 744$, and $a(1) = 196884$). Moreover, j is $\Gamma-$invariant, meaning that for any $\gamma \in \Gamma$,

$$j(\gamma\tau) = j(\tau),$$

where Γ acts on $\mathbb{H}$ via fractional linear transformation. In fact, any $\Gamma-$invariant holomorphic function on $\mathbb{H}$ which grows at most like q^{-N} for some N at ∞ must be a polynomial in j (see [13]), i.e. the space of such functions is simply $\mathbb{C}[j]$.

Using this information, one can define a positive definite scalar product on $\mathbb{R}[j]$ as follows: for two functions $f, g \in \mathbb{R}[j]$, let (f, g) denote the constant term of fg as a Laurent series in Δ. With respect to this scalar product one can produce a sequence of orthogonal polynomials $A_n(j)$. These are the polynomials discovered by Atkin.

Atkin's work on the subject was never published, but in [40] Kaneko and Zagier wrote up his results, and simplified some of his arguments. Though it is not obvious from this exposition, there exist relatively simple formulas for the Atkin polynomials, which can be obtained using the theory of modular forms. If we choose a slightly different normalization by setting $J = j/1728$ and $\mathcal{A}_n(J) = 1728^{-n} A_n(j)$ (the reason for this normalization will be made clear in Chapter 4), then the main result concerning Atkin polynomials is the following:

Theorem 1. *The Atkin polynomials $\mathcal{A}_n$ are determined in each of the following ways:*

i) Recursion relation:

$$\begin{aligned} \mathcal{A}_{n+1}(J) &= \left(J - \frac{144n^2 - 29}{2^3 3^2 \,(2n+1)\,(2n-1)}\right) \mathcal{A}_n(J) \\ &\quad - \frac{(12n-13)\,(12n-7)\,(12n-5)\,(12n+1)}{2^{10} 3^4 n(n-1)(2n-1)^2} \mathcal{A}_{n-1}(J) \end{aligned}$$

for $n \geq 2$, with initial values given by

$$\begin{aligned} \mathcal{A}_0(J) &= 1, \\ \mathcal{A}_1(J) &= J - \frac{5}{12}, \\ \mathcal{A}_2(J) &= J^2 - \frac{205}{216} J + \frac{935}{10368}. \end{aligned}$$

ii) Closed formula:

$$\mathcal{A}_n(J) = \sum_{i=0}^{n} J^{n-i} \sum_{\ell=0}^{i} (-1)^\ell \binom{-\frac{1}{12}}{i-\ell} \binom{-\frac{5}{12}}{i-\ell} \binom{n+\frac{1}{12}}{\ell} \binom{n-\frac{7}{12}}{\ell} \binom{2n-1}{\ell}^{-1}.$$

Kaneko and Zagier also prove that the $\mathcal{A}_n$ satisfy a certain fourth-order differential equation which can be used to construct the $\mathcal{A}_n$, but we will not use this result here.

Arguably the more important property of the Atkin polynomials concerns their zeros. Consider an elliptic curve E over a field of characteristic $p > 3$. Denote the Weierstrass model of E by the equation

$$y^2 = x^3 + ax + b$$

for some field elements a, b. Such a curve is said to be *supersingular* if the coefficient of x^{p-1} in $\left(x^3+ax+b\right)^{\frac{p-1}{2}}$ is nonzero. In fact, the condition of supersingularity is completely determined by the J-invariant of E, denoted

$$J(E) = \frac{4a^3}{4a^3+27b^2}.$$

This represents the usual j invariant scaled by a factor of $1/1728$ (see Chapter 4 for more on these definitions). Since there are only finitely many supersingular curves in $\overline{\mathbb{F}}_p$ ([68] has several explanations of this fact), one can define the so-called supersingular polynomial for the prime p by

$$ss_p(J) = \prod_{\substack{E/\overline{\mathbb{F}}_p \\ E \text{ supersingular}}} (J - J(E)) \in \mathbb{F}_p[J].$$

Inspired by a paper of R.A. Rankin (see [61]), Atkin proved the following result.

Theorem 2. *Let p be a prime number, $p \neq 2, 3$. Then*

$$ss_p(J) \equiv \mathcal{A}_{n_p}(J) \ mod\ p,$$

where

$$\begin{aligned} n_p &= \left\lfloor \frac{p-1}{12} \right\rfloor + \delta + \epsilon, \\ \epsilon &= \begin{cases} 0, & p \equiv 1, 7 \ mod\ 12, \\ 1, & p \equiv 5, 11 \ mod\ 12, \end{cases} \\ \delta &= \begin{cases} 0, & p \equiv 1, 5 \ mod\ 12, \\ 1, & p \equiv 7, 11 \ mod\ 12. \end{cases} \end{aligned}$$

In other words, the zeros of Atkin polynomials determine the J-invariants corresponding to supersingular elliptic curves.

The purpose of this thesis is to generalize Theorem 1 by interpreting the Atkin polynomials as but one set of orthogonal polynomials in an infinite family, which we name generalized Atkin polynomials, or Atkin-type polynomials. By investigating the zeros of these generalized Atkin polynomials, we can then deduce a generalization of Theorem 2 as well.

The basic idea is to consider generalizations of the J invariant. We do this by considering the Hecke triangle groups G_m; these are subgroups of $PSL_2(\mathbb{R})$ generated by the elements S and

$$T_m = \pm \begin{pmatrix} 1 & \lambda_m \\ 0 & 1 \end{pmatrix}$$

where $\lambda_m = 2\cos(\pi/m)$. One can consider the Hecke triangle groups for any integral $3 \leq m \leq \infty$; note that G_3 is simply the modular group Γ. Just as in the case of the modular group, for the Hecke triangle groups G_m one can construct an analogue of the J invariant, denoted J_m, which is G_m-invariant, holomorphic on $\mathbb{H}$, and has a simple pole at $i\infty$. In fact, these properties, along with the transformations

$$\begin{aligned} J_m\left(-e^{-\pi i/m}\right) &= 0, \\ J_m(i) &= 1, \\ J_m(i\infty) &= \infty \end{aligned}$$

essentially determine the function J_m uniquely.

The Hecke triangle groups were first studied by Hecke (see [27, 28]), and the triangle functions J_m have been the subject of additional study, mostly concerning the nature of their Fourier coefficients (see for example [46, 60, 77], or, more recently, [47]). As it turns out, one can modify the arguments of [40] to show that for each Hecke group G_m there exists a sequence of polynomials in the variable J_m which are orthogonal with respect to some scalar product. In fact, if we think of J_m as a holomorphic mapping of the hyperbolic triangle with vertices at $\left(i, -e^{-\pi i/m}, i\infty\right)$ to the upper half plane $\mathbb{H}$, we can generalize further, and consider triangle functions $J_{m,k}$ mapping the hyperbolic triangle with vertices at $\left(i, -e^{-\pi ik/m}, i\infty\right)$ to $\mathbb{H}$, where k is relatively prime to m and less than $m/2$ (this restriction is imposed since the sum of the angles of the triangle must be less than π). These triangle functions, it turns out, also give rise to orthogonal polynomials.

Taken altogether, this gives a sequence of orthogonal polynomials $\{\mathcal{A}_{n,m,k}(J)\}_{n=0}^{\infty}$ for any fixed $m \geq 3$ and any k with $1 \leq k < m/2$, $(k, m) = 1$. Our first result is the following generalization of Theoreom 1.

Theorem 3. *For each $m \geq 3$ and each k coprime to m and satisfying $1 \leq k < m/2$ there exists a family of orthogonal polynomials $\{\mathcal{A}_{n,m,k}(J)\}_{n=0}^{\infty}$ in the hyperbolic triangle functions $J(\tau) = J_{m,k}(\tau)$. These functions are orthogonal on $\mathbb{R}[J]$ with respect to a real valued weight function*

$$w_{m,k}(J) = \frac{-1}{2\pi\alpha_{m,k}J^{1/2}(1-J)^{1/2}F(\alpha_{m,k}, \beta_{m,k}; 1; 1/J)^2\Phi_{m,k}(J)}$$

where $\alpha_{m,k} = \frac{1}{2}\left(\frac{1}{2} - \frac{k}{m}\right)$, $\beta_{m,k} = \frac{1}{2} - \alpha_{m,k} = \frac{1}{2}\left(\frac{1}{2} + \frac{k}{m}\right)$*, and* $\Phi_{m,k}$ *is related to* J *via the equality*

$$\frac{2\pi i\tau}{\lambda_{m,k}} = \Phi_{m,k}(J),$$

for $\lambda_{m,k} = 2\cos\left(\pi k/m\right)$.

The polynomials $\mathcal{A}_{n,m,k}$ *are determined in the following ways:*

(i) By the recurrence relation

$$\mathcal{A}_{n+1,m,k}\left(J\right) = \left(J - a_{n,m,k}\right)\mathcal{A}_{n,m,k}\left(J\right) - b_{n,m,k}\mathcal{A}_{n-1,m,k}\left(J\right),$$

where

$$\begin{aligned} a_{n,m,k} &= \frac{4n^2 - 1 + 4\alpha_{m,k}\left(1 - \beta_{m,k}\right)}{2(2n-1)(2n+1)} \\ &= \frac{m^2\left(16n^2 - 1\right) - 8km + 4k^2}{8m^2(2n-1)(2n+1)} \end{aligned}$$

$$\begin{aligned} b_{n,m,k} &= \frac{\left(n + \alpha_{m,k}\right)\left(n - \beta_{m,k}\right)\left(n - 1 + \beta_{m,k}\right)\left(n - 1 - \alpha_{m,k}\right)}{4n(n-1)(2n-1)^2} \\ &= \frac{\left(4mn - 3m + 2k\right)\left(4mn - 5m + 2k\right)\left(4mn + m - 2k\right)\left(4mn - m - 2k\right)}{4^5 m^4 n(n-1)(2n-1)^2}. \end{aligned}$$

The recurrence is valid for $n \geq 2$*, with initial conditions*

$$\mathcal{A}_{0,m,k}\left(J\right) = 1,$$

$$\begin{aligned} \mathcal{A}_{1,m,k}\left(J\right) &= J - \beta_{m,k} \\ &= J - \frac{m+2k}{4m}, \end{aligned}$$

$$\begin{aligned} \mathcal{A}_{2,m,k}(J) &= J^2 + \frac{2\beta_{m,k}\left(\alpha_{m,k} - 1\right) - \alpha_m - 2}{3}J + \frac{\beta_{m,k}\left(1 - \alpha_{m,k}\right)\left(1 + \beta_{m,k}\right)}{6} \\ &= J^2 - \frac{21m^2 + 4mk + 4k^2}{24m^2}J + \frac{(m+2k)(3m+2k)(5m+2k)}{6\left(4m\right)^3}. \end{aligned}$$

(ii) By the closed formula

$$\mathcal{A}_{n,m,k}\left(J\right) = \sum_{i=0}^{n} J^{n-i}\left[\sum_{\ell=0}^{i}(-1)^{\ell}\binom{n + \alpha_{m,k}}{\ell}\binom{n - 1 + \beta_{m,k}}{\ell}\binom{2n-1}{\ell}^{-1}\binom{-\alpha_{m,k}}{i - \ell}\binom{-\beta_{m,k}}{i - \ell}\right].$$

Note Theorem 1 is an immediate Corollary of Theorem 3 in which $m = 3, k = 1$.

Once we construct this family of polynomials, it is natural to ask about their zeros. This question depends a bit on the value of m. When $m = 3, 4, 6, \infty$, the group G_m is arithmetic. In all other cases, G_m is non-arithmetic, i.e. G_m is not commensurable to any $PSL_2(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of some number field K. This was proven by Takeuchi in 1977. For a proof of this, see [72]; for general information on arithmetic groups, and more information on arithmetic triangle groups, see [39, 71, 73].

When G_m is arithmetic, the generalized Atkin polynomials still detect supersingularity. However, for $m = 4$ and $m = 6$, the polynomials are detecting the supersingularity of genus 2 hyperelliptic curves (see Section 4.1.1 for the general definition of a supersingular curve). As it turns out, the family of relevant curves for $m = 4$ was studied over a century ago in [78], and the family of relevant curves for $m = 6$ was studied around the same time in [30]. In all of these cases we only have one value of k ($k = 1$), so we frequently drop the subscript dependence on k and write $\mathcal{A}_{n,m,1} = \mathcal{A}_{n,m}$.

In the non-arithmetic case, the analogous result is not as tidy. In this setting we have more than one family of orthogonal polynomials to consider; to put it another way, for $m \neq 3, 4, 6, \infty$, the value of k need not be 1. So rather than looking at a single generalized Atkin polynomial modulo p, we must look at a product of generalized Atkin polynomials mod p, one for each k within some range of values. These values will not always be coprime to m, so we define

$$\mathcal{A}_{n,m,k} = \mathcal{A}_{n,\frac{m}{(k,m)},\frac{k}{(k,m)}}$$

in general. This is well defined since $k < m/2$ implies $\frac{m}{(k,m)} \geq 3$. Also, when m is odd it is possible for k to be zero; in this case, we have

$$\mathcal{A}_{n,m,0} = \mathcal{A}_{n,\infty,1}.$$

In the non-arithmetic case, the zeros of these polynomials are no longer detecting supersingular curves. Instead, they test whether or not some curve in a given family is ordinary. We defer the definition of ordinariness until Chapter 4, but for now the condition can simply be thought of as a weakening of the supersingularity condition.

With these modifications, we state the following result on the zeros of generalized Atkin polynomials.

Theorem 4. *Fix an $m > 3$ and a prime p satisfying $(p, 2m) = 1$. Consider the family $\mathcal{F}_m$ of hyperelliptic curves over $\overline{\mathbb{F}}_p$ given by a general equation of the form*

$$\begin{aligned} C:\ y^2 &= x^{1-\kappa_m}\left(x^{2g+2\kappa_m} - 2ax^{g+\kappa_m} + b\right) \\ &= x^{2g+1+\kappa_m} - 2ax^{g+1} + bx^{1-\kappa_m}, \end{aligned}$$

where

$$g = \frac{m}{(2,m)} - \kappa_m$$

and

$$\begin{aligned} \kappa_m &= \frac{(2m, m-2)}{(2,m)} - 1 \\ &= \begin{cases} 1, & m \equiv 2 \ mod \ 4, \\ 0, & otherwise. \end{cases} \end{aligned}$$

The coefficients a *and* b *are in* $\overline{\mathbb{F}}_p$ *and satisfy* $b - a^2 \neq 0$. *Let* $J = \frac{b}{b-a^2} = J_C$, *and define a polynomial in the variable* J *as follows:*

$$Nonord(J) := \prod_{\substack{C \in \mathcal{F}_m \\ C \ not \ ordinary}} (J - J_C).$$

Meanwhile, for each $1 \le i \le \lceil g/2 \rceil$, *define the value* $u = u_{p,i}$ *by*

$$\begin{aligned} u &= \left\lfloor \frac{(2i + \kappa_m - 1)\, p}{2\,(g + \kappa_m)} \right\rfloor \\ &= \frac{(2i + \kappa_m - 1)\, p}{2\,(g + \kappa_m)} - \frac{2j + \kappa_m - 1}{2\,(g + \kappa_m)} \end{aligned} \tag{1.0.1}$$

for a unique value of j *between 1 and* g*, in other words*

$$j = \left(i + \frac{\kappa_m - 1}{2} \right) p + \frac{1 - \kappa_m}{2} - (g + \kappa_m)\, u. \tag{1.0.2}$$

Define the values $\epsilon = \epsilon_{p,i}$, $\delta = \delta_{p,i}$, $k = k_{p,i}$, *and* $n = n_{p,i}$ *by*

$$\begin{aligned} \epsilon &= \left\lfloor \frac{j-1}{\lceil g/2 \rceil} \right\rfloor \\ &= \begin{cases} 0, & 1 \le j \le \lceil g/2 \rceil, \\ 1, & \lceil g/2 \rceil \le j \le g, \end{cases} \\ \delta &= u - 2 \lfloor u/2 \rfloor \\ &= \begin{cases} 0, & u \ even, \\ 1, & u \ odd, \end{cases} \\ k &= \frac{(2,m)}{2} \left| g + 1 - 2j \right| \\ &= (-1)^{\epsilon} \frac{(2,m)}{2} (g + 1 - 2j)\,, \end{aligned}$$

and

$$n = \lfloor u/2 \rfloor + \delta + \epsilon.$$

Finally, define a product of Atkin-type polynomials $\mathcal{P}_{m,p}(J)$ *by*

$$\mathcal{P}_{m,p}(J) = \prod_{i=1}^{\lceil g/2 \rceil} \mathcal{A}_{n_{p,i},m,k_{p,i}}(J).$$

Then

$$Nonord(J) \equiv \frac{\mathcal{P}_{m,p}(J)}{\left(\mathcal{P}_{m,p}, \mathcal{P}'_{m,p}\right)} \text{ mod } p.$$

Remark. In general, $\mathcal{P}_{m,p}$ may have multiple roots. We divide out by the GCD of $\mathcal{P}_{m,p}$ and its derivative because $Nonord(J)$ is square-free by definition. In the arithmetic cases, this is never an issue.

Also, the condition $b - a^2 \neq 0$ is analogous to the condition $\Delta \neq 0$ in the elliptic curve case where $m = 3$. In this case, $\Delta \neq 0$ is equivalent to the curve being nonsingular provided $p > 3$, but this is no longer true for general m, as the discriminant of the polynomials in the family $\mathcal{F}_m$ will always be divisible by b. However, as we will see, the case $b = 0$ is not difficult to analyze.

Because of all the parameters present in the statement of Theorem 4, it may be instructive to decompose the statement into separate cases, depending on the value of m. When $m \equiv 0$ mod 4, we have $g = m/2$ and the family $\mathcal{F}_m$ is given by curves of the form

$$y^2 = x\left(x^m - 2ax^{m/2} + b\right).$$

In this case, i ranges from 1 to $m/4$, and for each value of i we have

$$\begin{aligned} u &= \left\lfloor \frac{(2i-1)p}{m} \right\rfloor, \\ j &= ip - \frac{p-1}{2} - \frac{m}{2}u, \\ k &= \left| \frac{m}{2} + 1 - 2j \right|. \end{aligned}$$

Similarly, when $m \equiv 2$ mod 4, we have $g = m/2 - 1$ and the family $\mathcal{F}_m$ is given by curves of the form

$$y^2 = x^m - 2ax^{m/2} + b.$$

i ranges from 1 to $(m-2)/4$, and for each i we have

$$\begin{aligned} u &= \left\lfloor \frac{ip}{m/2} \right\rfloor, \\ j &= ip - \frac{m}{2}u, \\ k &= \left| \frac{m}{2} - 2j \right|. \end{aligned}$$

Finally, when $m > 3$ is odd, we have $g = m$ and the family $\mathcal{F}_m$ is given by curves of the form

$$y^2 = x\left(x^{2m} - 2ax^m + b\right).$$

Here i ranges from 1 to $(m+1)/2$, and for each value of i we have

$$\begin{aligned} u &= \left\lfloor \frac{(2i-1)p}{2m} \right\rfloor, \\ j &= ip - \frac{p-1}{2} - mu, \\ k &= \left| \frac{m+1}{2} - j \right|. \end{aligned}$$

In each case g denotes the value of the genus of the curve provided $b \neq 0$.

Specializing to the arithmetic cases gives us the following corollary, which can be more easily compared to Theorem 2.

Corollary 5. *(i) $m = 4$. Consider the family of curves $\mathcal{F}_4$ given by the equation*

$$y^2 = x^5 - 2ax^3 + bx \tag{1.0.3}$$

with $b - a^2 \neq 0$, and let p be an odd prime. Then the number of supersingular curves in $\mathcal{F}_4$ is finite over $\overline{\mathbb{F}}_p$ (up to isogeny), and

$$\begin{aligned} ss_{p,4}(J) &= \prod_{\substack{C/\overline{\mathbb{F}}_p \in \mathcal{F}_4 \\ C \text{ supersingular}}} (J - J(C)) \\ &\equiv \mathcal{A}_{n_p,4}(J) \bmod p, \end{aligned}$$

where $A_{n_p,4}$ is the degree n_p Atkin-type polynomial with $m = 4$, $J(C) = \frac{b}{b-a^2}$, and

$$\begin{aligned} n_p &= \left\lfloor \frac{p-1}{8} \right\rfloor + \delta + \epsilon, \\ \epsilon &= \begin{cases} 0, & p \equiv 1, 5 \ mod\ 8, \\ 1, & p \equiv 3, 7 \ mod\ 8, \end{cases} \\ \delta &= \begin{cases} 0, & p \equiv 1, 3 \ mod\ 8, \\ 1, & p \equiv 5, 7 \ mod\ 8. \end{cases} \end{aligned}$$

(ii) $m = 6$. Consider the family of curves $\mathcal{F}_6$ given by the equation

$$y^2 = x^6 - 2ax^3 + b \tag{1.0.4}$$

with $b - a^2 \neq 0$, and let p be an odd prime greater than 3. Then the number of supersingular curves in $\mathcal{F}_6$ is finite over $\overline{\mathbb{F}}_p$ (up to isogeny), and

$$\begin{aligned} ss_{p,6}(J) &= \prod_{\substack{C/\overline{\mathbb{F}}_p \in \mathcal{F}_6 \\ C\ supersingular}} (J - J(C)) \\ &\equiv \mathcal{A}_{n_p,6}(J) \ mod\ p, \end{aligned}$$

where $A_{n_p,6}$ is the degree n_p Atkin-type polynomial with $m = 6$, $J(C) = \frac{b}{b-a^2}$, and

$$\begin{aligned} n_p &= \left\lfloor \frac{p-1}{6} \right\rfloor + 2\epsilon, \\ \epsilon &= \begin{cases} 0, & p \equiv 1 \ mod\ 6, \\ 1, & p \equiv 5 \ mod\ 6. \end{cases} \end{aligned}$$

(iii) $m = \infty$. Consider the family of curves $\mathcal{F}_\infty$ given by the equation

$$y^2 = x^4 - 2ax^2 + b \tag{1.0.5}$$

with $b - a^2 \neq 0$, and let p be an odd prime. Then the number of supersingular curves in $\mathcal{F}_\infty$ is finite over $\overline{\mathbb{F}}_p$ (up to isogeny), and

$$\begin{aligned} ss_{p,\infty}(J) &= \prod_{\substack{C/\overline{\mathbb{F}}_p \in \mathcal{F}_\infty \\ C\ supersingular}} (J - J(C)) \\ &\equiv \mathcal{A}_{n_p,\infty}(J) \ mod\ p, \end{aligned}$$

where $A_{n_p,\infty}$ is the degree n_p Atkin-type polynomial with $m=\infty$, $J(C)=\frac{b}{b-a^2}$, and

$$\begin{aligned} n_p &= \left\lfloor \frac{p-1}{4} \right\rfloor + 2\epsilon, \\ \epsilon &= \begin{cases} 0, & p \equiv 1 \ mod\ 4, \\ 1, & p \equiv 3 \ mod\ 4. \end{cases} \end{aligned}$$

The distinction between ordinariness and supersingularity only becomes apparent when we begin to look at the non-arithmetic cases. In all cases, though, the zeros of Atkin-type polynomials provide information about the geometry of a corresponding curve.

This thesis is organized as follows. In Chapter 2 we prove Theorem 3. When $k=1$, the result can be proven using an argument analogous to the one appearing in [40]. For general k, instead of using the theory of modular forms for G_m, we approach the problem from the standpoint of hypergeometric functions. In fact, this approach is more general, and so we effectively give two proofs of the Theorem in the case $k=1$, equivalently the case when G_m is arithmetic.

Before proving Theorem 4, we provide some discussion of the family of curves in $\mathcal{F}_m$ in Chapter 3. In particular, we explain why these curves arise naturally, and prove a result on the correspondence between points in $G_m\backslash\mathbb{H}$ and isomorphism classes of curves in $\mathcal{F}_m$ which does not appear to exist in the literature. This material serves as further background, and is not necessary for the proof of the main result.

In Chapter 4 we prove Theorem 4. To do so, we need to first better understand what it means for a curve to be ordinary. We also give some basic examples and simple corollaries of the main result, and consider what happens in the simpler case when G_m is arithmetic.

Chapter 5 features further applications of these results. Inspired by [5], we prove a connection between the generalized Atkin polynomials and Jacobi polynomials. Motivated by a statement on the splitting of certain Jacobians in the $m=4$ and $m=6$ case mentioned in [9] we also investigate Jacobians of curves in $\mathcal{F}_m$. Finally, we reinterpret generalized Atkin polynomials from the standpoint of period functions and weakly holomorphic modular forms, and prove some new results on a certain family of modular integrals.

CHAPTER 2

Generalized Atkin Polynomials

In this chapter we construct the infinite family of sequences of Atkin-type polynomials introduced in the previous chapter, denoted by $\{\mathcal{A}_{n,m,k}(J)\}_{n=0}^{\infty}$ for some fixed $m \geq 3$ and $k < m/2$. Our goal is to provide a proof of Theorem 3. We first focus on the recursion formula. When $k = 1$, we can prove the formula by following the approach in [40]. For general k we apply the theory of hypergeometric functions, thereby giving us two proofs in the case $k = 1$. Once the recursion formula is proven, we use it to deduce the closed formula.

2.1. Generating function of the moments when $k = 1$

2.1.1. The proof of Kaneko and Zagier. A key observation in the proof of the closed form for the recurrence coefficients of the Atkin polynomials in [40] is the fact that the generating function of the moments associated to the inner product defined in the previous chapter is essentially a ratio of hypergeometric functions. To state this more precisely, let us first recall some definitions (see [40] for more details).

First, for a fixed positive even number ℓ, we define the weight ℓ Eisenstein series for $\Gamma = PSL_2(\mathbb{Z})$ by its $q-$expansion:

$$E_\ell(\tau) = 1 - \frac{2\ell}{B_\ell}\sum_{n=1}^{\infty}\left(\sum_{d|n} d^{k-1}\right)q^n,$$

where B_ℓ denotes the ℓth Bernoulli number. As in the introductory chapter, $q = e^{2\pi i\tau}$. When $\ell > 2$ (in particular, for $\ell = 4$ and $\ell = 6$), the above Eisenstein series is a modular form for Γ; in particular, it is holomorphic on $\mathbb{H}$, holomorphic near $i\infty$, and satisfies the following transformation rule:

$$E_\ell(\gamma\tau) = (c\tau + d)^\ell E_\ell(\tau), \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

When $\ell = 2$, the corresponding Eisenstein series is not modular, but does satisfy

$$E_2(\gamma\tau) = (c\tau + d)^2 E_2(\tau) + \frac{6}{\pi i}c(c\tau + d), \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \tag{2.1.1}$$

The functions E_2, E_4, E_6, and $\Delta = \frac{1}{1728}\left(E_4^3 - E_6^2\right)$ are related to one another via the following differential equations:

$$\begin{aligned} E_2' &= \frac{E_2^2 - E_4}{12} \\ E_4' &= \frac{E_2 E_4 - E_6}{3} \\ E_6' &= \frac{E_2 E_6 - E_4^2}{2} \\ \Delta' &= E_2 \Delta, \end{aligned}$$

where $'$ denotes differentiation with respect to $2\pi i\tau$.

We also recall the definition of the hypergeometric function ${}_2F_1\left(a, b; c; z\right)$. For $|z| < 1$ and c different from $0, -1, -2, \ldots$, we define ${}_2F_1\left(a, b; c; z\right)$ via the infinite series

$${}_2F_1\left(a, b; c; z\right) = \sum_{n=0}^{\infty} \frac{\left(a\right)_n \left(b\right)_n}{\left(c\right)_n n!} z^n,$$

where

$$\begin{aligned} \left(a\right)_k &= a(a+1)(a+2)\ldots(a+k-1) \\ &= \Gamma(a+k)/\Gamma(a) \end{aligned}$$

denotes the Pochhammer symbol. This function can be analytically continued to the entire complex plane, with a branch cut along the real axis from $z = 1$ to $z = \infty$. For more on hypergeometric functions, see Chapter 2 of [1].

Closely related is the function $F_1(a, b, z)$, defined initially for $|z| < 1$ via the infinite series

$$F_1\left(a, b; z\right) = \sum_{k=1}^{\infty} \frac{\left(a\right)_k \left(b\right)_k}{k!^2} \sum_{j=0}^{k-1} \left(\frac{1}{a+j} + \frac{1}{b+j} - \frac{2}{1+j} \right) z^k. \tag{2.1.2}$$

Like the hypergeometric function, $F_1(a, b, z)$ can be analytically continued.

These functions arise naturally in the study of solutions to the hypergeometric differential equation

$$z(1-z)y'' + [c - (a+b+1)z]y' - aby = 0. \tag{2.1.3}$$

Two linearly independent solutions to this differential equation when $c = 1$ (which will usually be the case for us) are given by ${}_2F_1\left(a, b; 1; z\right)$ and

$${}_2F_1\left(a, b; c; z\right) \log z + F_1(a, b, z).$$

Moreover, the inverse of the J function $J(\tau) = \frac{E_4^3(\tau)}{1728\Delta(\tau)}$ can be described in terms of these functions; as proven in [7] or [54] (or see [47] for a more recent treatment), if we consider the inverse to J and set $\Phi_3(J) = 2\pi i\tau$, then $\Phi_3(J)$ is given by

$$\Phi_3(J) = \log\left(\frac{1}{J}\right) + \frac{F_1\left(\frac{1}{12}, \frac{5}{12}; 1/J\right)}{{}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; 1/J\right)}.$$

Using the differential equations for the modular functions given above, along with a bit of complex analysis, Kaneko and Zagier first analyze the scalar product on $\mathbb{R}[j]$ which gives rise to the Atkin polynomials. In terms of the normalized function $J = j/1728$, their result yields the following information.

Proposition 6. *The following definitions of a scalar product on $\mathbb{R}[J]$ coincide:*

(i) $(f,g) =$ the constant term of fg as a Laurent series in Δ;

(ii) $(f,g) =$ the constant term of fgE_2E_4/E_6 as a Laurent series in J^{-1};

(iii) $(f,g) =$ the constant term of fgE_2 as a Laurent series in q;

(iv) $(f,g) = \frac{6}{\pi}\int_{\pi/3}^{\pi/2} f\left(e^{i\theta}\right) g\left(e^{i\theta}\right) d\theta$;

(v) $(f,g) = \int_0^1 f(J)g(J)w_3(J)dJ$, where

$$w_3(J) = \frac{-6}{\pi J^{1/2}(1-J)^{1/2}{}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; 1/J\right)^2 \Phi_3(J)}.$$

We refer to the weight function w_3 written above as the Atkin weight. Note that we are abusing notation slightly, since in (iv) f and g should be thought of as functions of θ, while in (v) they are viewed as functions of J. In practice, no confusion should arise. We omit the proof of this proposition, since we will prove a generalization of it below.

Thinking about the scalar product in terms of (v), one can then define the generating function $\mathcal{M}$ of the moments via the formal power series

$$\mathcal{M}(x) = \sum_{u=0}^{\infty} I_u x^u,$$

where

$$I_u = \int_0^1 J^u w(J) dJ.$$

The key ingredient needed to prove the recursion formula for the Atkin polynomials is then the fact that $\mathcal{M}$ satisfies

$$\mathcal{M}\left(\frac{1}{J}\right) = \frac{{}_2F_1\left(\frac{13}{12}, \frac{5}{12}; 1; \frac{1}{J}\right)}{{}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; \frac{1}{J}\right)}. \tag{2.1.4}$$

m	A_m
3	$1/1728$
4	$1/256$
5	$\sqrt{5}\left(2+\sqrt{5}\right)^{\sqrt{5}}/8000$
6	$1/108$
8	$\left(3+2\sqrt{2}\right)^{\sqrt{2}}/1024$
10	$\sqrt{5}\left(1+\sqrt{5}\right)^{\sqrt{5}}/\left(500\cdot 2^{\sqrt{5}}\right)$
∞	$1/64$

Table 1. Values of A_m for various m

From this, the classical theory of orthogonal polynomials combines with Gauss' contiguous relations for hypergeometric functions to give the recursion formula. To prove the recursion formula, therefore, one must first prove (2.1.4).

Kaneko and Zagier prove (2.1.4) by combining two steps:

(1) $\frac{1}{J}\mathcal{M}\left(\frac{1}{J}\right) = -\frac{d\log\Delta}{dJ}$,

(2) $\Delta = \frac{{}_2F_1(1/12,5/12;1;1/J)^{12}}{1728J}$.

These are the facts that we wish to generalize to the case of Hecke triangle groups G_m. To find the appropriate generalization, we first recall that for each $m \geq 3$ there exists a function $J_m(\tau)$ which conformally maps the interior of the hyperbolic triangle with vertices at $-e^{-\pi i/m}$, i, and $i\infty$ to the upper half plane, such that $J_m\left(-e^{-\pi i/m}\right) = 0$, $J_m(i) = 1$, and $J_m(i\infty) = \infty$. This function J_m is G_m invariant, is holomorphic on $\mathbb{H}$, and has a simple pole at $i\infty$. As in the case $m = 3$, $J_m(\tau)$ also has a q_m series expansion, where $q_m = e^{2\pi i\tau/\lambda_m}$, $\lambda_m = 2\cos(\pi/m)$, such that

$$J_m(\tau) = \frac{A_m}{q_m} + \sum_{n=0}^{\infty} a_{n,m} q^{nm},$$

where the $a_{n,m}$ are real numbers, and the constant A_m is determined by

$$\log A_m = -2\frac{\Gamma'}{\Gamma}(1) + \frac{\Gamma'}{\Gamma}\left(\frac{3}{4} - \frac{1}{2m}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{3}{4} + \frac{1}{2m}\right) - \pi\sec(\pi/m).$$

When $m = 3$ we have $A_3 = \frac{1}{1728}$ and $J_3(z)/A_3 = j(z)$; moreover, it was proven by Wolfart that A_m is transcendental except in the cases when G_m is arithmetic, i.e. except when $m = 3, 4, 6, \infty$ (see [77]). A table of some values of A_m for various m is presented in Table 1.

Also as in the case $m = 3$, if we consider the inverse function to $J_m(\tau)$ and set

$$\frac{2\pi i\tau}{\lambda_m} = \Phi_m(J),$$

then $\Phi_m(J)$ is a ratio of solutions to a certain hypergeometric differential equation (in fact, in many contexts this is how the function J_m is defined). In particular, Φ_m is given by

$$\Phi_m(J) = \log\left(\frac{A_m}{J}\right) + \frac{F_1\left(\alpha_m, \beta_m; 1/J\right)}{{}_2F_1\left(\alpha_m, \beta_m; 1; 1/J\right)},$$

where $\alpha_m = \frac{1}{2}\left(\frac{1}{2} - \frac{1}{m}\right)$, $\beta_m = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{m}\right)$ (note that for a fixed m, we shall sometimes omit the dependence on m and simply replace J_m by J). Such a function Φ_m is called a Schwarz triangle map; a thorough discussion of these maps can be found in [7]. In general, for a hyperbolic triangle with angles $\pi\nu$, $\pi\mu$, and $\pi\lambda$, the corresponding hypergeometric function arising in the inverse to the analogue of the J function has parameters

$$a = \frac{1}{2}\left(1 - \lambda - \mu - \nu\right) \tag{2.1.5}$$

$$b = \frac{1}{2}\left(1 - \lambda + \mu - \nu\right) \tag{2.1.6}$$

$$c = 1 - \lambda. \tag{2.1.7}$$

The parameters α_m, β_m, and 1 are determined by the angles $\pi/2, \pi/m, 0$.

With this notation, we introduce the following proposition:

Proposition 7. *Let $m \geq 3$ be an integer. Then there exists an analogue of the Atkin weight, which we denote w_m, given by*

$$w_m\left(J\right) = \frac{-1}{2\pi\alpha_m J^{1/2}(1-J)^{1/2}{}_2F_1\left(\alpha_m, \beta_m; 1; 1/J\right)^2 \Phi_m(J)} \tag{2.1.8}$$

on $[0,1]$, so that the generating function of the moments associated to w_m (denoted $\mathcal{M} = \mathcal{M}_m$) satisfies

$$\mathcal{M}\left(\frac{1}{J}\right) = \frac{{}_2F_1\left(\alpha_m + 1, \beta_m; 1; \frac{1}{J}\right)}{{}_2F_1\left(\alpha_m, \beta_m; 1; \frac{1}{J}\right)}. \tag{2.1.9}$$

To prove this proposition, we must prove analogues of steps 1 and 2 for G_m. We will then show how the recurrence equation for the generalized Atkin polynomials with $k = 1$ follows from this proposition, by using Gauss' contiguous relations.

2.1.2. Proving an analogue of step 1. Before we formulate and prove an analogue of step 1, we need to generalize the scalar product on $\mathbb{R}[J]$ given in the introduction. This, in turn, requires some background on modular forms for G_m, which we briefly review now (see [28] for more details).

On G_m there are two canonical modular forms, typically denoted f_0 and f_i of weights $\frac{4}{m-2}$ and $\frac{2m}{m-2}$, respectively. Of course, f_0 and f_i depend on m, but we suppress this dependence in the notation. In the case $m = 3$ these modular forms are the familiar Eisenstein series E_4 and E_6, and as in the case $m = 3$, the modular forms f_0 and f_i satisfy

$$\begin{aligned} f_0(T_m z) &= f_0(z) \\ f_i(T_m z) &= f_i(z) \\ f_0(Sz) &= (-iz)^{\frac{4}{m-2}} f_0(z), \\ f_i(Sz) &= -(-iz)^{\frac{2m}{m-2}} f_i(z). \end{aligned}$$

Of particular interest is the canonical cusp form Δ_m on G_m. For $m = 3$ we defined the usual cusp form $\Delta_3 = \Delta$ via the relations

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = \frac{E_4^3}{j}.$$

In the same way, we can define Δ_m via the relations

$$\Delta_m = A_m \left(f_0^m - f_i^2 \right) = \frac{A_m f_0^m}{J_m}. \tag{2.1.10}$$

Δ_m is then a cusp form of weight $\frac{4m}{m-2}$ for G_m.

We can use Δ_m to define an analogue of the weight 2 Eisenstein series E_2 in the case $m = 3$. One way to define the weight 2 Eisenstein series is via the formula

$$\frac{d\Delta(\tau)}{d\tau} = 2\pi i E_2(\tau)\Delta(\tau).$$

In other words, the weight 2 Eisenstein series for $\Gamma(1)$ is essentially the logarithmic derivative of Δ. For general m, we can use a similar equation to define a function $E_{2,m}$ by

$$E_{2,m} := \frac{\Delta_m'}{\Delta_m},$$

where $'$ denotes differentiation with respect to $2\pi i\tau/\lambda_m$ (this ensures that the q_m expansion of $E_{2,m}$ has leading coefficient 1). By differentiating the functional equation $\Delta_m\left(\frac{az+b}{cz+d}\right) = (-i(cz+d))^{\frac{4m}{m-2}}\Delta_m(z)$, it follows that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_m$,

$$E_{2,m}(\gamma z) = (cz+d)^2 E_{2,m}(z) + \frac{2m\lambda_m}{\pi i(m-2)} c(cz+d). \tag{2.1.11}$$

We also need some information on the derivatives of f_0, f_i, Δ_m, $E_{2,m}$, and J_m. This information is provided by the following lemma, and will be used heavily throughout the next two sections.

LEMMA 8. *Fix a whole number $m \geq 3$. Then the following equalities hold:*

$$\Delta_m' = \Delta_m E_{2,m}, \;\; E_{2,m}' = \tfrac{m-2}{4m}\left(E_{2,m}^2 - f_0^{m-2}\right)$$

$$f_0' = \tfrac{E_{2,m}f_0 - f_i}{m}, \;\; f_i' = \tfrac{E_{2,m}f_i - f_0^{m-1}}{2}, \;\; J_m' = -\tfrac{J_m f_i}{f_0},$$

where $'$ denotes differentiation with respect to $2\pi i\tau/\lambda_m$.

Proof. The first equality holds by definition of $E_{2,m}$. For the second, it follows from (2.1.11) that $E_{2,m}'(\tau) - \frac{m-2}{4m}E_{2,m}^2(\tau)$ is modular on G_m of weight 4. Since the space of modular forms on G_m of weight k has dimension at most $\left\lfloor \frac{k(m-2)}{4m} \right\rfloor + 1$ (a more precise dimension statement can be found in Chapter 5), the space of modular forms of weight 4 has dimension 1, which means that

$$E_{2,m}' - \frac{m-2}{4m}E_{2,m}^2 = cf_0^{m-2}$$

for some c, since f_0^{m-2} has weight 4. Considering the first term of the q_m series expansion, it follows that $c = -\frac{m-2}{4m}$.

A similar argument works for the derivatives of f_0 and f_i. In particular, from the modularity relation for f_0 it follows that $f_0' - \frac{1}{m}E_{2,m}f_0$ is modular of weight $\frac{2m}{m-2}$, so by dimension restrictions must be a multiple of f_i, and from the q_m expansion the constant must be $-1/m$. Similarly, from the modularity relation for f_i it follows that $f_i' - \frac{1}{2}E_{2,m}f_i$ is modular on G_m of weight $\frac{4(m-1)}{m-2}$, so by dimension restrictions must be a multiple of f_0^{m-1}, and from the q_m expansion the constant must be $-1/2$. The last equation follows from the previous ones, along with the second equality in (2.1.10). □

The desired generalized scalar product is now provided by the following analogue of Proposition 6.

Proposition 9. *The following definitions of a scalar product $(\cdot,\cdot)_m$ on $\mathbb{R}[J_m]$ are equivalent:*

(i) $(f,g)_m$ = the constant term of fg as a Laurent series in Δ_m,

(ii) $(f,g)_m$ = the constant term of $fgE_{2,m}f_0/f_i$ as a Laurent series in J^{-1},

(iii) $(f,g)_m$ = the constant term of $fgE_{2,m}$ as a Laurent series in q_m;

(iv) $(f,g)_m = \frac{2m}{\pi(m-2)}\int_{\pi/m}^{\pi/2} f\left(e^{i\theta}\right) g\left(e^{i\theta}\right) d\theta$;

(v) $(f,g)_m = \int_0^1 f(J)\, g(J)\, w_m(J)\, dJ$, where w_m is given by (2.1.8).

Proof. The first three scalar products are equivalent since, by Lemma 8, we have the equalities

$$\frac{d\Delta_m(\tau)}{\Delta_m(\tau)} = \frac{2\pi i}{\lambda_m}E_{2,m}(\tau)d\tau = E_{2,m}(\tau)\frac{dq_m}{q_m} = -\frac{f_0E_{2,m}}{f_i}\frac{dJ}{J}.$$

So it suffices to show that (iii) and (iv) are equivalent, and that (iv) and (v) are equivalent. To prove the first equivalence, let $\mathfrak{F}_m(Y)$ denote a truncated fundamental domain for $G_m\backslash\mathbb{H}$ for some fixed Y, in other words

$$\mathfrak{F}_m(Y) = \{z = x + iy \in \mathbb{H} : |z| \geq 1, |x| \leq \lambda_m, y \leq Y\},$$

with G_m-equivalent points on the boundary identified. We want to integrate $f(\tau)g(\tau)E_{2,m}(\tau)$ around the boundary of $\mathfrak{F}_m(Y)$.

By Cauchy's Theorem, the integral must be zero, since $E_{2,m}$ is holomorphic on $\mathbb{H}$. On the other hand, the integrals along the left and right hand sides of the contour cancel, and the integral along the top is equal to $\lambda_m(f,g)_m$. Splitting the integral along the bottom circular arc into a contour from $e^{\pi i/m}$ to i and from i to $-e^{-\pi i/m}$, and using (2.1.11),

$$\begin{aligned}
\lambda_m(f,g)_m &= -\int_{\rho_m}^{i} f(\tau)g(\tau)E_{2,m}(\tau)d\tau - \int_{i}^{\overline{\rho_m}} f(\tau)g(\tau)E_{2,m}(\tau)d\tau \\
&= -\int_{\rho_m}^{i} f(\tau)g(\tau)\left[E_{2,m}(\tau) - \tau^{-2}E_{2,m}(-1/\tau)\right]d\tau \\
&= \frac{2m\lambda_m}{\pi i(m-2)}\int_{\rho_m}^{i} f(\tau)g(\tau)\frac{d\tau}{\tau} \\
&= \frac{2m\lambda_m}{\pi(m-2)}\int_{\pi/m}^{\pi/2} f\left(e^{i\theta}\right)g\left(e^{i\theta}\right)d\theta
\end{aligned}$$

under the change of variables $\tau = e^{i\theta}$. Dividing out by λ_m then gives the result.

For the equivalence between (iv) and (v), we observe that for θ in the range $[\pi/m, \pi/2]$,

$$\frac{2\pi i}{\lambda_m}e^{i\theta} = \Phi_m\left(J_m\left(e^{i\theta}\right)\right),$$

so that if we view $J_m = J$ as a variable on $[0,1]$, we have

$$\begin{aligned}
d\theta &= \frac{-\lambda_m}{2\pi e^{i\theta}}\Phi_m'(J)dJ. \\
&= \frac{\Phi_m'(J)}{i\Phi_m(J)}dJ.
\end{aligned}$$

We now wish to find an expression for $\Phi_m'(J)$. By the definition of Φ_m, we see that Φ_m is a ratio of two functions y_1 and y_2, where

$$\begin{aligned}
y_1(J) &= {}_2F_1\left(\alpha_m, \beta_m; 1; 1/J\right), \\
y_2(J) &= {}_2F_1\left(\alpha_m, \beta_m; 1; 1/J\right)\log\left(\frac{A_m}{J}\right) + F_1\left(\alpha_m, \beta_m; 1/J\right).
\end{aligned}$$

If we replace $1/J$ by w, we see that y_1 and y_2 viewed as functions of w satisfy the hypergeometric differential equation (2.1.12) with $a = \alpha_m$, $b = \beta_m$, and $c = 1$.

Now, it is a general fact that if y_1 and y_2 are two solutions to a second order differential equation of the form

$$y'' + P(w)y' + Q(w)y = 0,$$

then the Wronskian $G = y_1 y_2' - y_1' y_2$ satisfies $G' = -P(w)G$, so that

$$G(w) = Ke^{-\int P(w)dw}$$

for some constant K. In particular, for y_1 and y_2 given above, we have

$$P(w) = \frac{1 - 3w/2}{w(1-w)} = \frac{1}{w} + \frac{1}{2\,(w-1)}$$

so that

$$G = \frac{K}{w(1-w)^{1/2}}$$

and

$$\begin{aligned} \frac{d\Phi_m}{dw} &= \frac{y_1 \frac{dy_2}{dw} - \frac{dy_1}{dw} y_2}{y_1^2} \\ &= \frac{K}{w(1-w)^{1/2} {}_2F_1\left(\alpha_m, \beta_m; 1; w\right)^2}. \end{aligned}$$

Furthermore, by considering the limiting behavior as $z \to 0$, it follows that $K = 1$. Therefore, by the chain rule,

$$\begin{aligned} \Phi'(J) &= \frac{d\Phi}{dw}\frac{dw}{dJ} \\ &= \frac{-1}{J^{1/2}(J-1)^{1/2} {}_2F_1\left(\alpha_m, \beta_m; 1; 1/J\right)^2}, \end{aligned}$$

so that

$$\frac{2m}{\pi(m-2)} d\theta = w_m(J)dJ,$$

with $w_m(J)$ as defined by (2.1.8). Note the limits of integration with respect to J are 0 and 1 by basic properties of the function J_m. □

With a firmer understanding of the scalar product for general m, we now state and prove a proposition giving an analogue of step 1.

Proposition 10. *The generating function $\mathcal{M} = \mathcal{M}_m$ of the moments satisfies*

$$\frac{1}{J_m}\mathcal{M}\left(\frac{1}{J_m}\right) = -\frac{d \log \Delta_m}{dJ_m}.$$

PROOF. By Proposition 9, we see that the kth moment of the weight w_m is the coefficient of J_m^{-k-1} in $\frac{E_{2,m} f_0}{J_m f_i}$ as a series in J_m^{-1}; in other words,

$$\frac{1}{J_m}\mathcal{M}\left(\frac{1}{J_m}\right) = \frac{E_{2,m} f_0}{f_i J_m}.$$

On the other hand, we see that the right hand side is equal to $-\frac{d \log \Delta_m}{dj_m}$ by Lemma 8. □

2.1.3. Proving an Analogue of Step 2. An analogue of step 2 is a consequence of the following proposition:

PROPOSITION 11. $f_0 = {}_2F_1\left(\alpha_m, \beta_m; 1; 1/J_m\right)^{\frac{4}{m-2}}$.

PROOF. In general, the two independent solutions to the hypergeometric differential equation

$$z(1-z)\frac{d^2y}{dz^2} + [1-(a+b+1)z]\frac{dy}{dz} - aby = 0 \tag{2.1.12}$$

are given by the hypergeometric function ${}_2F_1(a,b;1;z)$ and ${}_2F_1(a,b;1;z)\log z + F_1(a,b;z)$, where F_1 is given by (2.1.2). Let g_0 be a function satisfying (2.1.12) with $a = \alpha_m$, $b = \beta_m$, and let $g(z) = g_0(1/J_m(z))$. Using the equations from Lemma 8, a straightforward calculation shows that g satisfies the following differential equation:

$$\left(\frac{\lambda_m}{2\pi i}\right)^2 \frac{d^2g}{dz^2} + \left(\frac{1}{2} - \frac{1}{m}\right)\frac{\lambda_m}{2\pi i}\left(\frac{f_i}{f_0} - E_{2,m}\right)\frac{dg}{dz} + \frac{f_0^{m-2}}{4J_m}\left(\frac{1}{4} - \frac{1}{m^2}\right) g = 0.$$

Another calculation shows that $f_0^{\frac{m-2}{4}}$ satisfies the same differential equation. It follows that

$$\begin{aligned} f_0(z)^{\frac{m-2}{4}} &= A{}_2F_1\left(\alpha_m, \beta_m; 1; 1/J_m(z)\right) \\ &\quad + B\left(F_1\left(\alpha_m, \beta_m; 1/J_m(z)\right) - {}_2F_1\left(\alpha_m, \beta_m; 1; 1/J_m(z)\right)\log J_m(z)\right) \end{aligned} \tag{2.1.13}$$

for certain constants A and B.

To determine the values of A and B, note that the left hand side of (2.1.13) is constant at $i\infty$, so B must equal 0 to compensate for the fact that $J_m(i\infty) = \infty$, so the logarithmic term diverges. Since the first term in the q_m expansion of $f_0(z)$ is 1, this then gives us that $A = 1$, and so the result holds. □

Combining this proposition with (2.1.10), we see that

$$\Delta_m = \frac{A_m f_0^m}{J_m} = \frac{A_m}{J_m}{}_2F_1\left(\alpha_m, \beta_m; 1; 1/J_m\right)^{\frac{4m}{m-2}}, \tag{2.1.14}$$

and this is the desired analogue of Step 2.

We also obtain the following corollary immediately from this description of the function Δ_m along with (2.1.8):

Corollary 12. *The generalized Atkin weight $w_m(J)$ can be written as*

$$w_m(J) = \frac{-2mA_m^{2\alpha_m}}{\pi(m-2)J^{1/2+2\alpha_m}(1-J)^{1/2}\Delta_m\left(\frac{\lambda_m}{2\pi i}\Phi_m(J)\right)^{2\alpha_m}\Phi_m(J)}.$$

We will return to this description of the weight in Chapter 5.

2.1.4. Completing the Proof of Proposition 7.

Let's now combine the results from Propositions 10 and 11 to complete the proof of Proposition 7. This is analogous to the procedure carried out in [40], but for sake of completeness we include the argument here.

Combining the two propositions, we see that

$$\begin{aligned}\frac{1}{J_m}\mathcal{M}\left(\frac{1}{J_m}\right) &= -\frac{d\log\Delta_m}{dJ_m}\\ &= -d\left(\log\left(\frac{A_m}{J_m}{}_2F_1\left(\alpha_m,\beta_m;1;1/J_m\right)^{\frac{4m}{m-2}}\right)\right)/dJ_m\\ &= \frac{1}{J_m}\left(1+\frac{{}_2F_1'\left(\alpha_m,\beta_m;1;1/J_m\right)}{\alpha_m J_m {}_2F_1\left(\alpha_m,\beta_m;1;1/J_m\right)}\right),\end{aligned}$$

since $\alpha_m^{-1} = \frac{4m}{m-2}$. By Gauss' contiguous relations (see [1] for more details), we also know

$$(2.1.15)\qquad {}_2F_1'\left(\alpha_m,\beta_m;1;1/J_m\right) = \alpha_m J_m\left({}_2F_1\left(\left(\alpha_m+1,\beta_m;1;1/J_m\right)\right) - {}_2F_1\left(\alpha_m,\beta_m;1;1/J_m\right)\right).$$

Substituting this into the above expression and simplifying, we then get

$$\mathcal{M}\left(\frac{1}{J_m}\right) = \frac{{}_2F_1\left(\alpha_m+1,\beta_m;1;\frac{1}{J_m}\right)}{{}_2F_1\left(\alpha_m,\beta_m;1;\frac{1}{J_m}\right)},$$

as desired.

2.2. Generating function of the moments when $k \neq 1$

2.2.1. Defining a J function for $k \neq 1$.

Throughout the previous section we assumed $k = 1$. In other words, we only considered the triangle function J_m mapping $\left\{-e^{-\pi i/m}, i, i\infty\right\}$ to $\{0,1,\infty\}$. We made this simplification to exploit the theory of modular forms for the Hecke groups G_m.

However, we will need to define scalar products on $\mathbb{R}[J]$ for a larger family of triangle functions J whenever m differs from 3, 4, 6, or ∞. In other words, in the general setting there is no longer only one hyperbolic triangle to consider. In fact, as discussed in [10, 64] one can construct a triangle for each element $\sigma_k \in \mathrm{Gal}\left(\mathbb{Q}(\cos(\pi/m)/\mathbb{Q}\right)$ by mapping the vertex $-e^{-\pi i/m}$ to the vertex $\sigma_k\left(-e^{-\pi i/m}\right) = -e^{-\pi ik/m}$ for some k coprime to m. Equivalently, one can view σ as acting on the generator T_m of the Hecke triangle group G_m

via

$$\sigma\begin{pmatrix}1 & \lambda_m\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & \sigma\left(\lambda_m\right)\\ 0 & 1\end{pmatrix}.$$

This mapping is not injective; in fact, for Hecke triangle groups it is two to one. The number of distinct triangles that can be formed with this construction is equal to $\varphi(m)/2$, and without loss of generality we may assume $k < m/2$. As usual φ denotes Euler's Phi function, which counts the number of positive integers less than m and coprime to m. In particular, note that $\varphi(m) = 2$ if and only if $m = 3, 4, 6$. For example, when $m = 5$ there are two triangles: one with angles $\left(0, \frac{\pi}{5}, \frac{\pi}{2}\right)$, and one with angles $\left(0, \frac{2\pi}{5}, \frac{\pi}{2}\right)$ (for more on the $m = 5$ case, see [64]).

Corresponding to any such triangle there is a triangle function, analogous to the function J_m we have already considered (see [10] for more details). For any $m \geq 3$ and any k coprime to m, we denote this J function by $J_{m,k}$. If, as will sometimes be the case, m and k are not coprime, then we set $J_{m,k} = J_{\frac{m}{(m,k)},\frac{k}{(m,k)}}$, which is well defined when $k < m/2$. We also define $J_{m,0} = J_\infty$, because the case $k = 0$ will arise when m is odd. Where no confusion will occur, we simply denote the triangle function as J.

The triangle functions $J_{m,k}$ map $\left\{-e^{-\pi ik/m}, i, i\infty\right\}$ to $\{0, 1, \infty\}$ for any $3 \leq m \leq \infty$ and any $1 \leq k \leq m/2$ relatively prime to m. However, when the angles of the triangle are not of the form π/n for some positive integer n (with n possibly infinite), the corresponding group is no longer discrete. As a consequence, the J functions $J_{m,k}$ can no longer be automorphic with respect to the group $G_{m,k}$ generated by

$$\begin{aligned} S &= \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\\ T_{m,k} &= \begin{pmatrix}1 & \lambda_{m,k}\\ 0 & 1\end{pmatrix},\end{aligned}$$

where $\lambda_{m,k} = 2\cos(\pi k/m)$. In fact, there can be no nonconstant automorphic forms with respect to such a group.

Before discussing the inner product in this setting, we need a better understanding of the relationship between the various functions $J_{m,k}$ for m fixed and k coprime to m. The most important point is the fact that if we set $r = \varphi(m)/2$, then there exists a complex analytic embedding $F : \mathbb{H} \to \mathbb{H}^r$ extending the action of G_m on $\mathbb{H}$. This well-known result was was proven in [10] and is discussed in several related papers, see for example [3, 11, 65]. The embedding F is determined by r mappings f_k satsifying

$$f_k\left(\gamma\tau\right) = \gamma_k f_k(\tau)$$

$$\begin{tikzcd}
\mathfrak{F}_m \arrow[rr, "\varphi_k"] \arrow[dr, shift left, "J_m"] & & \mathfrak{F}_{m,k} \\
& \mathbb{C} \arrow[ul, shift left, "\frac{\lambda_m}{2\pi i}\Phi_m"] \arrow[ur, "\frac{\lambda_{m,k}}{2\pi i}\Phi_{m,k}"'] &
\end{tikzcd}$$

FIGURE 2.2.1. Commutative diagram for φ_k

for any $\gamma \in G_m$, where $\gamma_k = \sigma_k(\gamma)$ and on both sides the group action is given by fractional linear transformation.

The functions f_k can be described explicitly. For each fixed k, consider a biholomorphic mapping from the interior of the hyperbolic triangle with vertices $\left\{-e^{-\pi i/m}, i, i\infty\right\}$ to the interior of the hyperbolic triangle with vertices $\left\{-e^{-\pi ik/m}, i, i\infty\right\}$. Such a mapping can be constructed using Schwarz triangle maps and their inverses. In particular, the function $J_m = J_{m,1}$ maps the first triangle to the upper half plane, and, in analogue with the Schwarz triangle functions Φ_m, the function

$$\Phi_{m,k}(w) = \log\left(\frac{A_{m,k}}{w}\right) + \frac{F_1\left(\alpha_{m,k}, \beta_{m,k}; 1/w\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; 1/w\right)},$$

maps the upper half plane to the second triangle. Here the parameters $\alpha_{m,k}, \beta_{m,k}$, and $A_{m,k}$ are given by

$$\alpha_{m,k} = \frac{1}{2}\left(\frac{1}{2} - \frac{k}{m}\right), \tag{2.2.1}$$

$$\beta_{m,k} = \frac{1}{2}\left(\frac{1}{2} + \frac{k}{m}\right), \tag{2.2.2}$$

$$\log A_{m,k} = -2\frac{\Gamma'}{\Gamma}(1) + \frac{\Gamma'}{\Gamma}\left(1 - \alpha_{m,k}\right) + \frac{\Gamma'}{\Gamma}\left(1 - \beta_{m,k}\right) - \pi \sec\left(\pi\left(\beta_{m,k} - \alpha_{m,k}\right)\right).$$

These reduce to the previous formulas when $k = 1$. As before, $\Phi_{m,k}$ is a ratio of solutions to the hyperelliptic differential equation, but with the relevant angle changed from π/m to $k\pi/m$. Calculation of the term $\log A_{m,k}$ can be found in [7].

This mapping between the two triangles extends holomorphically to the boundary, and by Schwarz reflection can be reflected across the line from i to $i\infty$, creating a biholomorphic mapping from the fundamental domain $\mathfrak{F}_m$ of $G_m\backslash\mathbb{H}$ to the domain $\mathfrak{F}_{m,k}$, a set consisting of the points

$$\{z : |z| > 1, |\mathrm{Re} z| < \cos(\pi k/m)\}$$

along with the left boundary and the left half of the bottom boundary. As usual, the boundary of $\mathfrak{F}_{k,m}$ consists of pairs of points that are equivalent under the action of $G_{m,k}$.

This gives us a mapping φ_k such that the diagram in Figure 2.2.1 commutes. In particular, $J_{m,k}$ is related to the inverse of $\Phi_{m,k}$ via the identity

$$\Phi_{m,k}\left(J_{m,k}(\tau)\right) = \frac{2\pi i\tau}{\lambda_{m,k}}.$$

Since we can tessellate the upper half plane by images of $\mathfrak{F}_m$ under G_m, one can continue to apply Shwarz reflection to extend φ_k to an analytic mapping on the entire upper half plane; this extension is the map f_k described above. More details on this construction can be found in Section 3 of [10]. For the purposes of understanding the inner product in this more general setting, we need only concern ourselves with the mapping φ_k determined by the commutative diagram above, i.e.

$$\varphi_k\left(\tau\right) = \frac{\lambda_{m,k}}{2\pi i}\Phi_{m,k}\left(J_m(\tau)\right)$$

for $\tau \in \mathfrak{F}_m$.

2.2.2. Construction of the inner product. With a better understanding of the functions $J_{m,k}$ and how they relate to one another, we can now prove the following analogue of Proposition 7 in the case of general k.

Proposition 13. *Let $m \geq 3$ be an integer, and let $k < m/2$ be a fixed positive integer coprime to m. Then there exists an analogue of the Atkin weight, which we denote $w_{m,k}$, given by*

$$w_{m,k}\left(J\right) = \frac{-1}{2\pi\alpha_{m,k}J^{1/2}(1-J)^{1/2}{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;1/J\right)^2\Phi_{m,k}(J)} \tag{2.2.3}$$

on $[0,1]$, so that the generating function of the moments associated to $w_{m,k}$ (denoted $\mathcal{M} = \mathcal{M}_{m,k}$) satisfies

$$\mathcal{M}_{m,k}\left(\frac{1}{J}\right) = \frac{{}_2F_1\left(\alpha_{m,k}+1,\beta_{m,k};1;\frac{1}{J}\right)}{{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J}\right)}. \tag{2.2.4}$$

We prove this result by constructing an inner product for which the condition on $\mathcal{M}_{m,k}$ is clearly satisfied. For fixed k and m coprime with $k < m/2$, we begin by defining an inner product $(\cdot,\cdot)_{m,k}$ on $\mathbb{R}\left[J_{k,m}\right] = \mathbb{R}\left[J\right]$ by setting

$$\begin{aligned}(f,g)_{m,k} \quad &= \quad \text{the constant term of } f(J)g(J)\frac{{}_2F_1\left(\alpha_{m,k}+1,\beta_{m,k};1;\frac{1}{J}\right)}{{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J}\right)} \\ &\qquad \text{as a Laurent series in } J^{-1}.\end{aligned}$$

Notice that this is completely analogous to definition (ii) of the scalar product $(\cdot,\cdot)_m$ from Proposition 9, since by Lemma 8, (2.1.14), and (2.1.15), we have =

$$\begin{aligned}\frac{E_{2,m}f_0}{f_i} &= -\frac{\Delta'_m}{\Delta}\frac{J}{J'} \\ &= 1+\frac{{}_2F'_1\left(\alpha_m,\beta_m;1;\frac{1}{J}\right)}{{}_2F_1\left(\alpha_m,\beta_m;1;\frac{1}{J}\right)} \\ &= \frac{{}_2F_1\left(\alpha_m+1,\beta_m;1;\frac{1}{J}\right)}{{}_2F_1\left(\alpha_m,\beta_m;1;\frac{1}{J}\right)}.\end{aligned}$$

With this definition, the inner product of J^n and 1 is simply the coefficient of J^{-n} in the Laurent series expansion of

$$\frac{{}_2F_1\left(\alpha_{m,k}+1,\beta_{m,k};1;\frac{1}{J}\right)}{{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J}\right)},$$

so that this ratio is the generating function of the moments, when viewed as a function of $1/J$.

The more difficult part of the proof is showing that this inner product agrees with the one given in terms of the weight $w_{m,k}$. To prove this, we follow the type of argument used in Proposition 9. We begin by considering a truncated domain

$$\mathfrak{F}_{m,k}(Y)=\{z=x+iy\in\mathfrak{F}_{m,k}: y\le Y\}$$

and suppose we want to integrate the function

$$\text{(2.2.5)}\qquad \frac{\lambda_{m,k}}{2\pi i}f\left(J_{m,k}(z)\right)g\left(J_{m,k}(z)\right)\frac{J'_{m,k}(z)}{J_{m,k}(z)}\frac{{}_2F_1\left(\alpha_{m,k}+1,\beta_{m,k};1;\frac{1}{J_{m,k}(z)}\right)}{{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J_{m,k}(z)}\right)}$$

over the boundary of $\mathfrak{F}_{m,k}(Y)$, oriented clockwise. Here the symbol $'$ denotes the usual differentiation with respect to the variable z.

We first claim this integral equals 0. To see this, note that the ratio of hypergeometric functions

$$\frac{{}_2F_1\left(a+1,b;c;z\right)}{{}_2F_1\left(a,b;c;z\right)}$$

is analytic in $\mathbb{C}\backslash[1,\infty)$ (see, for example, Theorem 1.5 of [44]). This means (2.2.5) is analytic everywhere inside and on the boundary of $\mathfrak{F}_{m,k}(Y)$ except the bottom arc, since $J_{m,k}$ maps the circular arc from $-e^{-\pi ik/m}$ to i to the interval from 0 to 1. Similarly, it maps the circular arc from $e^{\pi i/m}$ to i to the same interval, since even though $J_{m,k}$ is not automorphic in general, for z on the circular arc between $-e^{-\pi ik/m}$

to i, there exists τ on the bottom arc of the boundary of $\mathfrak{F}_m$ such that

$$\begin{aligned} J_{m,k}\left(-\frac{1}{z}\right) &= J_{m,k}\left(Sz\right) \\ &= J_{m,k}\left(S\varphi_k(\tau)\right) \\ &= J_{m,k}\left(\varphi_k\left(S\tau\right)\right) \\ &= J_m\left(S\tau\right) \\ &= J_m(\tau) = J_{m,k}(z). \end{aligned}$$

In particular, if we consider the modified domain $\mathfrak{F}_{m,k}(Y,\epsilon)$ obtained by requiring that $|z| > 1+\epsilon$, then the integral of (2.2.5) around the boundary of $\mathfrak{F}_{m,k}(Y,\epsilon)$ equals zero for any $\epsilon > 0$ by Cauchy's Theorem. Taking $\epsilon \to 0$ then gives the desired result for the original integral.

Similar to the calculation above, even though $J_{m,k}$ is not automorphic with respect to $\sigma_k\left(G_m\right) = G_{m,k}$ for $k \neq 1$, the above commutative diagram still ensures that if z is on the left hand side of the boundary of $\mathfrak{F}_{m,k}(Y)$,

$$J_{m,k}\left(z+\lambda_{m,k}\right) = J_{m,k}(z), \tag{2.2.6}$$

so that the integral along the left and right hand sides of the boundary cancel each other out. Therefore, just as in the proof of Proposition 9, the integral consists of two opposite pieces: one along the path

$$\mathcal{C}_1 = \left\{x+iY : |x| \leq \lambda_{m,k}/2\right\},$$

and one along the path

$$\mathcal{C}_2 = \left\{z = x+iy : |z| = 1, |x| \leq \lambda_{m,k}/2\right\}.$$

For the integral along the top, we transform from the z variable to the variable $J_{k,m} = J$ (we will continue to abuse notation slightly, by letting J represent either a function or a variable, as suits our needs). This change of variables transforms the integral to

$$\frac{\lambda_{m,k}}{2\pi i}\int_{J_{m,k}(\mathcal{C}_1)} f(J)g(J)\frac{{}_2F_1\left(\alpha_{m,k}+1,\beta_{m,k};1;\frac{1}{J_{m,k}(z)}\right)}{J\,{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J_{m,k}(z)}\right)}dJ.$$

In these new variables, note that the path of integration is now a loop, because of (2.2.6). Moreover, since $\mathcal{C}_1$ and $\mathcal{C}_2$ are disjoint, and $J_{m,k}$ maps $\mathcal{C}_2$ two-to-one to the interval $[0,1]$, we see that the closed path $J_{m,k}\left(\mathcal{C}_1\right)$ avoids the branch cut of the ratio of hypergeometric functions. Therefore, by the residue theorem the value of this integral is just the coefficient of J^{-1} in

$$\lambda_{m,k} f(J) g(J) \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J_{m,k}(z)}\right)}{J {}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J_{m,k}(z)}\right)};$$

in other words, the integral along $\mathcal{C}_1$ is precisely $-\lambda_{m,k}\left(f,g\right)_{m,k}$.

The integral along the bottom needs to be treated more carefully, since we are essentially integrating along the branch cut of the ratio of hypergeometric functions. Note, however, that as in the $k=1$ case we can still split $\mathcal{C}_2$ into two pieces which are mapped onto each other via $z \mapsto -\frac{1}{z}$. In particular, we can write

$$\begin{aligned}
\lambda_{m,k}\left(f,g\right)_{m,k} &= \frac{\lambda_{m,k}}{2\pi i} \int_{\mathcal{C}_2} f\left(J(z)\right) g\left(J(z)\right) \frac{J'(z)}{J(z)} \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J(z)}\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right)} dz \\
&= \frac{\lambda_{m,k}}{2\pi i} \int_{e^{\pi i k/m}}^{i} f\left(J(z)\right) g\left(J(z)\right) \frac{J'(z)}{J(z)} \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J(z)}\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right)} dz \\
&- \frac{\lambda_{m,k}}{2\pi i} \int_{-e^{-\pi i k/m}}^{i} f\left(J(z)\right) g\left(J(z)\right) \frac{J'(z)}{J(z)} \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J(z)}\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right)} dz.
\end{aligned}$$

On the second integral, we make the transformation $z \mapsto -\frac{1}{z}$. Since we've already seen that $J_{m,k}(z) = J_{m,k}\left(-\frac{1}{z}\right)$ on $\mathcal{C}_2$, we see that

$$J'(z) = \left(J\left(-\frac{1}{z}\right)\right)' = \frac{1}{z^2} J'\left(-\frac{1}{z}\right),$$

which tells us the second integral is the same as

$$-\frac{\lambda_{m,k}}{2\pi i} \int_{e^{\pi i k/m}}^{i} f(J(z)) g(J(z)) \frac{J'(z)}{J(z)} \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J(-z^{-1})}\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(-z^{-1})}\right)} dz.$$

Here is where we must be careful. Since we are integrating along the branch cut, it is not true that ${}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(-z^{-1})}\right)$ and ${}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right)$ must be equal. In order to proceed from here, we need to make use of the following proposition.

Proposition 14. *For $z \in \mathcal{C}_2$, the following transformation law holds:*

$$\text{(2.2.7)} \qquad {}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(-z^{-1})}\right) = -iz {}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right).$$

We will prove this proposition below; for now, let's see how this proposition allows us to complete the proof of Proposition 13.

To simplify the notation, for the remainder of this section we set

$$\begin{aligned} F(z) &= {}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J(z)}\right), \\ F_+(z) &= {}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J(z)}\right). \end{aligned}$$

If we know that (2.2.7) holds, then by taking the logarithmic derivative of both sides with respect to z, we see that

$$\frac{\left(F\left(-\frac{1}{z}\right)\right)'}{F\left(-\frac{1}{z}\right)} = \frac{\left(F\left(z\right)\right)'}{F\left(z\right)} + \frac{1}{z}.$$

On the other hand, by the contiguous relation (2.1.15) we know

$$\frac{F_+(z)}{F(z)} = 1 - \frac{J(z)}{\alpha_{m,k}J'(z)}\frac{F'(z)}{F\left(z\right)},$$

which in turn implies

$$\frac{F_+\left(-\frac{1}{z}\right)}{F\left(-\frac{1}{z}\right)} = 1 - \frac{J(z)}{\alpha_{m,k}J'(z)}\frac{\left(F\left(-\frac{1}{z}\right)\right)'}{F\left(-\frac{1}{z}\right)}.$$

Combining these three equalities then gives us the following:

$$\frac{F_+\left(-\frac{1}{z}\right)}{F\left(-\frac{1}{z}\right)} = \frac{F_+\left(z\right)}{F\left(z\right)} - \frac{J(z)}{\alpha_{m,k}\tau J'(z)}.$$

Returning to our above calculation of the original intergal,

$$\begin{aligned} (f,g)_{m,k} &= \frac{1}{2\pi i}\int_{e^{\pi ik/m}}^{i} f\left(J(z)\right)g\left(J(z)\right)\frac{J'(z)}{J(z)}\left[\frac{F_+(z)}{F(z)} - \frac{F_+\left(-\frac{1}{z}\right)}{F\left(-\frac{1}{z}\right)}\right]dz \\ &= \frac{1}{2\pi i\alpha_{m,k}}\int_{e^{\pi ik/m}}^{i} f\left(J(z)\right)g\left(J(z)\right)\frac{dz}{z}. \end{aligned}$$

Now using the fact that

$$z = \frac{\lambda_{k,m}}{2\pi i}\Phi_{m,k}\left(J\right),$$

and by changing variables once more, we obtain

$$(f,g)_{m,k} = \frac{1}{2\pi i\alpha_m}\int_0^1 f(J)g(J)\frac{\Phi'_{m,k}(J)}{\Phi_{m,k}(J)}dJ.$$

The proof that

$$w_{m,k}(J) = \frac{1}{2\pi i\alpha_{m,k}}\frac{\Phi'_{m,k}(J)}{\Phi_{m,k}(J)} \tag{2.2.8}$$

is unchanged from the case where $k = 1$, so this completes the proof of Proposition 13 assuming Proposition 14 is true.

We now turn our attention towards proving Proposition 14. This requires an understanding of how the hypergeometric function transforms when we move across the branch cut. We will need a few transformation laws for hypergeometric functions; a fairly exhaustive list of them can be found in the tables at the end of Section 395 in [7].

The triangle function $J_{m,k}(z)$ maps the triangle with vertices $\left\{-e^{-\pi ik/m}, i, i\infty\right\}$ to the upper half plane, and maps the boundary of this triangle to the real axis. By Schwarz reflection it maps the triangle with vertices $\left\{e^{\pi ik/m}, i, i\infty\right\}$ to the lower half plane, again mapping the boundary to the real axis. Therefore, $1/J_{m,k}(z)$ flips the ranges of these two functions, so that as z approaches the circular arc from $-e^{-\pi ik/m}$ to i from above, $1/J_{m,k}(z)$ approaches the branch cut of $\frac{F_+(z)}{F(z)}$ from below, while as z approaches the circular arc from $e^{\pi ik/m}$ to i from above, $1/J_{m,k}(z)$ approaches the branch cut of $\frac{F_+(z)}{F(z)}$ from above.

To understand the behavior near the branch cut, we recall the following transformation rule:

$$\begin{aligned} {}_2F_1\left(a,b;c;w\right) &= \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}{}_2F_1\left(a,b;a+b+1-c;1-w\right) \\ &+ \frac{\Gamma(c)\Gamma(a+b-c)}{\Gamma(a)\Gamma(b)}(1-w)^{c-a-b}{}_2F_1\left(c-a,c-b;1+c-a-b;1-w\right), \end{aligned}$$

provided $c \neq a+b$. In particular, for the case $a = \alpha_{m,k}$, $b = \beta_{m,k}$, $c = 1$, since $\alpha_{m,k} + \beta_{m,k} = \frac{1}{2}$, we can write this transformation as

$$\begin{aligned} {}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;w\right) &= \frac{\Gamma(1/2)}{\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)}{}_2F_1\left(\alpha_{m,k},\beta_{m,k};\frac{1}{2};1-w\right) \\ &+ \frac{\Gamma(-1/2)}{\Gamma\left(\alpha_{m,k}\right)\Gamma\left(\beta_{m,k}\right)}\left(1-w\right)^{1/2}{}_2F_1\left(1-\alpha_{m,k},1-\beta_{m,k};\frac{3}{2};1-w\right). \end{aligned}$$

For $|w-1|<1$, the hypergeometric functions on the right hand side of the above formula will both be analytic, so the branching behavior of the left hand side is completely determined by the presence of the $(1-w)^{1/2}$ term on the right. From this it follows that, restricted to the set $|w-1|<1$, if we set $w = u+iv$, we have

$$\begin{aligned} &\lim_{v\to 0^+} {}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;w\right) + \lim_{v\to 0^-} {}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;w\right) \\ &= \frac{\Gamma(1/2)}{\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)}{}_2F_1\left(\alpha_{m,k},\beta_{m,k};\frac{1}{2};1-u\right). \end{aligned}$$

By our above analysis of how $J_{m,k}$ behaves as z approaches $\mathcal{C}_2$ from above, the above equality in terms of $J_{m,k}$ becomes

$$F(z) + F\left(-\frac{1}{z}\right) = \frac{2\Gamma(1/2)}{\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)}{}_2F_1\left(\alpha_{m,k},\beta_{m,k};\frac{1}{2};1-\frac{1}{J_{m,k}(z)}\right) \tag{2.2.9}$$

for z on $\mathcal{C}_2$.

This doesn't give us our desired transformation, but it does bring us one step closer. Next we apply another transformation to handle the hypergeometric function on the right hand side of (2.2.9). Namely, we have the following identity in the special case $c = a + b$:

$$ {}_2F_1\left(a, b; a+b; 1-w\right) = C\,{}_2F_1\left(a, b; 1; w\right) + D\left({}_2F_1\left(a, b; 1; w\right)\log w + F_1\left(a, b; w\right)\right), $$

where

$$\begin{aligned} C &= \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\left(2\frac{\Gamma'}{\Gamma}(1) - \frac{\Gamma'}{\Gamma}(a) - \frac{\Gamma'}{\Gamma}(b)\right), \\ D &= -\frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}, \end{aligned}$$

and we recall $F_1(a, b, z)$ is given by (2.1.2). More transformations like this will be given in the next chapter.

To apply the above transformation to the right hand side of (2.2.9) we must multiply everything by

$$\frac{2\Gamma(1/2)}{\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)}.$$

The effect of this on the constants C and D is easily obtained. For D,

$$\begin{aligned} & \frac{2\Gamma(1/2)}{\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)}D \\ = & -\frac{2\Gamma(1/2)^2}{\Gamma\left(\alpha_{m,k}\right)\Gamma\left(1-\alpha_{m,k}\right)\Gamma\left(\beta_{m,k}\right)\Gamma\left(1-\beta_{m,k}\right)} \\ = & -\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right), \end{aligned}$$

since $\Gamma(1/2) = \sqrt{\pi}$ and

$$\Gamma(x)\Gamma(1-x) = \pi\csc\left(\pi x\right). \tag{2.2.10}$$

Similarly, for C observe that

$$\begin{aligned} & 2\frac{\Gamma'}{\Gamma}(1) - \frac{\Gamma'}{\Gamma}\left(\alpha_{m,k}\right) - \frac{\Gamma'}{\Gamma}\left(\beta_{m,k}\right) \\ = & \; 2\frac{\Gamma'}{\Gamma}(1) - \frac{\Gamma'}{\Gamma}\left(1-\alpha_{m,k}\right) - \frac{\Gamma'}{\Gamma}\left(1-\beta_{m,k}\right) + \pi\cot\left(\pi\alpha_{m,k}\right) + \pi\cot\left(\pi\beta_{m,k}\right) \\ = & -\log A_{m,k} - \pi\sec\left(\pi\left(\beta_{m,k}-\alpha_{m,k}\right)\right) + \pi\cot\left(\pi\alpha_{m,k}\right) + \pi\cot\left(\pi\beta_{m,k}\right) \\ = & -\log A_{m,k} + \pi\sec\left(\pi\alpha_{m,k}\right)\sec\left(\pi\beta_{m,k}\right), \end{aligned}$$

where we have applied the logarithmic derivative of (2.2.10) in the first step, and the definition of $\log A_{m,k}$ in the second step. The third step then follows from basic trigonometry, along with the fact that $\alpha_{m,k}+\beta_{m,k}=1/2$. This means that

$$C=-\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)\log A_{m,k}+2.$$

We are now ready to rewrite the right hand side of (2.2.9). By what we have just shown, it must equal

$$\begin{aligned}
&\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)\left[\left(\pi\sec\left(\pi\alpha_{m,k}\right)\sec\left(\pi\beta_{m,k}\right)-\log A_{m,k}\right)F(z)\right.\\
&\left.+F(z)\log J_{m,k}(z)-F_1\left(\alpha_{m,k},\beta_{m,k};\frac{1}{J_{m,k}(z)}\right)\right]\\
=\;&-\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)F(z)\left[\Phi_{m,k}\left(J_{m,k}(z)\right)-\pi\sec\left(\pi\alpha_{m,k}\right)\sec\left(\pi\beta_{m,k}\right)\right]\\
=\;&-\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)F(z)\left[\frac{2\pi iz}{\lambda_{m,k}}-\pi\sec\left(\pi\alpha_{m,k}\right)\sec\left(\pi\beta_{m,k}\right)\right].
\end{aligned}$$

Therefore, (2.2.9) becomes

$$\begin{aligned}
F\left(-\frac{1}{z}\right)&=-\frac{2}{\pi}\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)F(z)\left[\frac{2\pi iz}{\lambda_{m,k}}-\pi\sec\left(\pi\alpha_{m,k}\right)\sec\left(\pi\beta_{m,k}\right)\right]-F(z)\\
&=\frac{-4i\sin\left(\pi\alpha_{m,k}\right)\sin\left(\pi\beta_{m,k}\right)}{\lambda_{m,k}}zF(z)\\
&=-izF(z),
\end{aligned}$$

again by basic trigonometry and the fact that $\lambda_{m,k}=2\cos\left(\pi\left(\beta_{m,k}-\alpha_{m,k}\right)\right)$. This completes the proof of Proposition 14.

One could obtain generalizations of some of the other formulations of the inner product $(\cdot,\cdot)_m$ given in Proposition 9, but this will not be necessary in what follows. The above argument works equally well in the case $k=1$, so actually we have provided two proofs of Theorem 7; one from the perspective of modular forms, one from the perspective of hypergeometric functions. The former proof is a clearer analogue of the result in [40], though is not as general as the result proven here.

In any event, with the proof complete we can safely conclude that regardless of the value of k, the generating function associated to the moments of $w_{m,k}$ is a ratio solutions to the hypergeometric differential equation, and this is what will allow us to prove the first part of Theorem 3.

2.3. The recurrence relation for generalized Atkin polynomials

The proof of the first part of Theorem 3 uses several well-known results; references to relevant proofs are provided throughout. We assume a certain degree of familiarity with the basic theory of orthogonal polynomials. There are many excellent references on the subject - see, for example, [14, 35, 69].

To begin, we use the following result from the study of orthogonal polynomials, proven in [40]. Suppose we have a weight w on some interval $[a, b]$ and a corresponding sequence of orthogonal polynomials $\pi_n(x)$. These polynomials will then satisfy a three-term recurrence of the form

$$\pi_{n+1}(x) = (x - a_n)\pi_n(x) - b_n\pi_{n-1}(x).$$

Let the sequence of moments given by this weight be denoted by $\{I_n\}_{n=0}^{\infty}$, and let $\mathcal{M}(x)$ denote the generating function corresponding to these moments. If we define the numbers $\{\lambda_n\}_{n=1}^{\infty}$ by the equation

$$\mathcal{M}(x) = I_0 + I_1 x + I_2 x^2 + \ldots = \frac{I_0}{1 - \frac{\lambda_1 x}{1 - \frac{\lambda_2 x}{1 - \ldots}}}, \tag{2.3.1}$$

then

$$\begin{aligned} a_n &= \lambda_{2n} + \lambda_{2n+1} && (2.3.2)\\ b_n &= \lambda_{2n}\lambda_{2n-1}. && (2.3.3) \end{aligned}$$

In the case of the weights determined by the inner products defined above, we know that regardless of the value of k,

$$\mathcal{M}\left(\frac{1}{J}\right) = \frac{{}_2F_1\left(\alpha_{m,k}+1, \beta_{m,k}; 1; \frac{1}{J}\right)}{{}_2F_1\left(\alpha_{m,k}, \beta_{m,k}; 1; \frac{1}{J}\right)} = \sum_{n=0}^{\infty} \frac{I_{n,m,k}}{J^n}, \tag{2.3.4}$$

and therefore, to determine the coefficients $\{\lambda_{n,m,k}\}_{n=1}^{\infty}$ appearing in (2.3.1), it suffices to determine the continued fraction expansion of the ratio of hypergeometric functions in the above equation.

By Gauss's contiguous relations, it is well-known (see [1] for example) that

$$\frac{{}_2F_1(a, b; c; z)}{{}_2F_1(a+1, b; c; z)} = 1 - \frac{zb}{c}\frac{1}{\frac{{}_2F_1(a+1,b;c;z)}{{}_2F_1(a+1,b+1;c+1;z)}},$$

and the contiguous relations can also be used to give the continued fraction expansion of $\frac{{}_2F_1(a+1,b;c;z)}{{}_2F_1(a+1,b+1;c+1;z)}$. It follows that

$$\frac{{}_2F_1(a+1, b; c; z)}{{}_2F_1(a, b; c; z)} = \frac{1}{1 - \frac{\lambda_1 z}{1 - \frac{\lambda_2 z}{1 - \ldots}}},$$

where

$$\begin{aligned} \lambda_1 &= \frac{b}{c},\\ \lambda_{2n} &= \frac{(a+n)(c-b+n-1)}{(c+2n-2)(c+2n-1)},\\ \lambda_{2n+1} &= \frac{(b+n)(c-a-1+n)}{(c+2n-1)(c+2n)}. \end{aligned}$$

Therefore, using the fact that $\alpha_{m,k} + \beta_{m,k} = 1/2$, the ratio in (2.1.9) has corresponding coefficients $\lambda_{n,m}$ given by

$$\lambda_{n,m,k} = \begin{cases} \beta_{m,k}, & n = 1 \\ \left(\frac{1}{2} + \frac{(-1)^n \alpha_{m,k}}{n}\right)\left(\frac{1}{2} + \frac{(-1)^n \alpha_{m,k}}{n-1}\right), & n > 1. \end{cases}$$

The formulas for $a_{n,m,k}$ and $b_{n,m,k}$ then follow from the fact that $\alpha_{m,k} = \frac{m-2k}{4m}$, $\alpha_{m,k} + \beta_{m,k} = \frac{1}{2}$, and the identities (2.3.2) and (2.3.3).

The formulas for $\mathcal{A}_{n,m,k}$ for $n \leq 2$ can be found directly by using the theory of orthogonal polynomials. Given the moments, one can determine the orthogonal polynomials by computing determinants. For $\mathcal{A}_{1,m,k}$ and $\mathcal{A}_{2,m,k}$, the relevant expressions are

$$\begin{aligned} \mathcal{A}_{1,m,k}(J) &= \det\begin{pmatrix} 1 & I_{1,m,k} \\ 1 & J \end{pmatrix}, \\ \mathcal{A}_{2,m,k}(J) &= \frac{\det\begin{pmatrix} 1 & I_{1,m,k} & I_{2,m,k} \\ I_{1,m,k} & I_{2,m,k} & I_{3,m,k} \\ 1 & J & J^2 \end{pmatrix}}{\det\begin{pmatrix} 1 & I_{1,m,k} \\ I_{1,m,k} & I_{2,m,k} \end{pmatrix}}. \end{aligned}$$

The first few moments $I_{n,k,m}$ can be computed directly from the first few terms in the formal power series expansion of the right hand side of (2.3.4). In particular, we find that

$$\begin{aligned} I_{1,m,k} &= \beta_{m,k} \\ I_{2,m,k} &= \frac{1}{2}\beta_{m,k}\left((\alpha_{m,k}+1)(\beta_{m,k}+1) - 2\alpha_{m,k}\beta_{m,k}\right) \\ I_{3,m,k} &= \frac{1}{6}\beta_{m,k}\left(\alpha_{m,k}^2\left(2\beta_{m,k}^2 - 3\beta_{m,k}+1\right) - 3\alpha_{m,k}\left(\beta_{m,k}^2-1\right) + \beta_{m,k}^2 + 3\beta_{m,k} + 2\right). \end{aligned}$$

The first part of Theorem 3 then follows after simplification.

2.4. The closed formula for generalized Atkin polynomials

To prove part (ii) of Theorem 3, we first introduce four polynomials via the equations

$$
\begin{aligned}
J^{n}{}_2F_1\left(\alpha_{m,k},\beta_{m,k};1;\frac{1}{J}\right) &= U^{0}_{n,m,k}\left(J\right)+O\left(\frac{1}{J}\right),\\
J^{n-1}\left(J-1\right){}_2F_1\left(1-\beta_{m,k},1-\alpha_{m,k};1;\frac{1}{J}\right) &= U^{1}_{n,m,k}\left(J\right)+O\left(\frac{1}{J}\right),\\
\left(J-1\right)^{n}{}_2F_1\left(\alpha_{m,k},1-\beta_{m,k};1;\frac{1}{1-J}\right) &= V^{0}_{n,m,k}\left(J\right)+O\left(\frac{1}{J}\right),\\
J\left(J-1\right)^{n-1}{}_2F_1\left(\beta_{m,k},1-\alpha_{m,k};1;\frac{1}{1-J}\right) &= V^{1}_{n,m,k}\left(J\right)+O\left(\frac{1}{J}\right).
\end{aligned}
$$

One can think of these polynomials as truncated hypergeometric series.

The relationship between the polynomials $U^{\delta}_{n,m,k}$ and $V^{\epsilon}_{n,m,k}$ and the Atkin-type polynomials $\mathcal{A}_{n,m,k}$ is determined by the following proposition, which serves as a generalization of Proposition 4 of [40].

Proposition 15. *The Atkin-type polynomials $\mathcal{A}_{n,m,k}$ have the following expressions in terms of the polynomials introduced above:*

$$
\begin{aligned}
\mathcal{A}_{n,m,k}\left(J\right) &= \sum_{\ell=0}^{n}(-1)^{\ell}\binom{n+\alpha_{m,k}}{\ell}\binom{n+\beta_{m,k}-1}{\ell}\binom{2n-1}{\ell}^{-1}U^{0}_{n-\ell,m,k}\left(J\right),\\
\mathcal{A}_{n,m,k}\left(J\right) &= \sum_{\ell=0}^{n}(-1)^{\ell}\binom{n-\alpha_{m,k}-1}{\ell}\binom{n-\beta_{m,k}}{\ell}\binom{2n-1}{\ell}^{-1}U^{1}_{n-\ell,m,k}\left(J\right),\\
\mathcal{A}_{n,m,k}\left(J\right) &= \sum_{\ell=0}^{n}\binom{n+\alpha_{m,k}}{\ell}\binom{n-\beta_{m,k}}{\ell}\binom{2n-1}{\ell}^{-1}V^{0}_{n-\ell,m,k}\left(J\right),\\
\mathcal{A}_{n,m,k}\left(J\right) &= \sum_{\ell=0}^{n}\binom{n-\alpha_{m,k}-1}{\ell}\binom{n+\beta_{m,k}-1}{\ell}\binom{2n-1}{\ell}^{-1}V^{1}_{n-\ell,m,k}\left(J\right).
\end{aligned}
$$

Proof. We prove the first of these formulas; the proof of the remaining three is similar. Denote the right hand side of the first formula by $\mathcal{A}^{0}_{n,m,k}\left(J\right)$. For $n\leq 2$, one verifies the equality $\mathcal{A}_{n,m,k}=\mathcal{A}^{0}_{n,m,k}$ directly. Therefore, by the first part of Theorem 3, it suffices to show that

$$
\mathcal{A}^{0}_{n+1,m,k}\left(J\right)=\left(J-a_{n,m,k}\right)\mathcal{A}^{0}_{n,m,k}\left(J\right)-b_{n,m,k}\mathcal{A}^{0}_{n-1,m,k}\left(J\right), \tag{2.4.1}
$$

where the recurrence coefficients $a_{n,m,k}$ and $b_{n,m,k}$ are identical to the recurrence coefficients for the Atkin-type polynomials, as given in the theorem.

Write $\mathcal{A}^{0}_{n,m,k}\left(J\right)$ as

$$
\mathcal{A}^{0}_{n,m,k}\left(J\right)=\sum_{\ell=0}^{n}c_{m,k}(n,\ell)U^{0}_{\ell,m,k}\left(J\right).
$$

By direct computation, and using the fact that

$$\binom{n+x}{n} = (-1)^n \binom{-x-1}{n},$$

one finds that

$$c_{m,k}(n,0) \quad = \quad (-1)^n \binom{-\alpha_{m,k}-1}{n}\binom{-\beta_{m,k}}{n}\binom{2n-1}{n}^{-1}, \tag{2.4.2}$$

$$c_{m,k}(n,\ell) \quad = \quad c_{m,k}(n,0)\binom{n}{\ell}\binom{-n}{\ell}\binom{-\beta_{m,k}}{\ell}^{-1}\binom{-\alpha_{m,k}-1}{\ell}^{-1}. \tag{2.4.3}$$

Also, by definition of $U^0_{\ell,m,k}$,

$$JU^0_{\ell,m,k} - U^0_{\ell+1,m,k} = -\binom{-\alpha_{m,k}}{\ell+1}\binom{-\beta_{m,k}}{\ell+1}.$$

Combining these facts, (2.4.1) becomes

$$\begin{aligned}&\sum_{\ell=0}^{n}\left[c_{m,k}(n+1,\ell) - c_{m,k}(n,\ell-1) + a_{n,m,k}c_{m,k}(n,\ell) + b_{n,m,k}c_{m,k}(n-1,\ell)\right] U^0_{\ell,m,k} \\ &+\sum_{\ell=0}^{n}\binom{-\alpha_{m,k}}{\ell+1}\binom{-\beta_{m,k}}{\ell+1}c_{m,k}(n,\ell).\end{aligned} \tag{2.4.4}$$

To complete the proof, we need to show this expression is 0 whenever $n \geq 2$. Using the formulas for the recurrence relations $a_{n,m,k}$ and $b_{n,m,k}$ along with the relations

$$\begin{aligned} c_{m,k}(n+1,\ell) &= -\frac{(n+\ell)\,(n+\beta_{m,k})\,(n+\alpha_{m,k}+1)}{2n\,(n-\ell+1)\,(2n+1)}c_{m,k}(n,\ell), \\ c_{m,k}(n,\ell+1) &= \frac{(\ell-n)\,(n+\ell)}{(\ell+\beta_m)\,(\ell+1+\alpha_m)}c_{m,k}(n,\ell), \end{aligned}$$

one can show that the term in brackets in (2.4.4) is 0 for $\ell \geq 1$, and, by setting $c_{m,k}(n,-1) = 0$, for $\ell = 0$ the term in brackets equals

$$\begin{aligned} & c_{m,k}(n+1,0) + a_{n,m,k}c_{m,k}(n,0) + b_{n,m,k}c_{m,k}(n-1,0) \\ = \quad & c_{m,k}(n,0)\left[-\frac{(n+\beta_{m,k})\,(n+\alpha_{m,k}+1)}{2(n+1)(2n+1)} + a_{n,m,k} - b_{n,m,k}\frac{2n(2n-1)}{(n-1+\beta_{m,k})\,(n+\alpha_{m,k})}\right] \\ = \quad & c_{m,k}(n,0)\left[-\frac{(n+\beta_{m,k})\,(n+\alpha_{m,k}+1)}{2(n+1)(2n+1)} + \frac{4n^2-1+4\alpha_{m,k}(1-\beta_{m,k})}{2(2n-1)(2n+1)} - \frac{(n-\beta_{m,k})\,(n-\alpha_{m,k}-1)}{2(n-1)(2n-1)}\right] \\ = \quad & c_{m,k}(n,0)\frac{\alpha_{m,k}\,(1-\beta_{m,k})}{n^2-1}. \end{aligned}$$

Therefore, we may rewrite (2.4.4) as

$$\begin{aligned} & c_{m,k}(n,0)\frac{\alpha_{m,k}\left(1-\beta_{m,k}\right)}{n^2-1}+\sum_{\ell=0}^{n}\binom{-\alpha_m}{\ell+1}\binom{-\beta_m}{\ell+1}c_m(n,\ell) \\ = \;& \alpha_{m,k}c_{m,k}(n,0)\left[\frac{1-\beta_{m,k}}{n^2-1}+\sum_{\ell=0}^{n}\frac{\beta_{m,k}+\ell}{(\ell+1)^2}\binom{n}{\ell}\binom{n}{-\ell}\right] \\ = \;& \frac{\alpha_{m,k}c_{m,k}(n,0)}{n^2-1}\left[1-\beta_{m,k}+\sum_{\ell=0}^{n}\left(\beta_{m,k}+n-\ell\right)\binom{n+1}{\ell}\binom{1-n}{n-\ell+1}\right] \\ = \;& \frac{\alpha_{m,k}c_{m,k}(n,0)}{n^2-1}\left[\sum_{\ell=0}^{n+1}\binom{1-n}{n-\ell+1}\left[\left(\beta_{m,k}-1\right)\binom{n+1}{\ell}-(n+1)\binom{n}{\ell}\right]\right], \end{aligned}$$

where we have used the change of variables $\ell \to n-\ell$ in moving from the second line to the third. Finally, we observe that the sum in the above expression represents the coefficient of the x^{n+1} term in

$$(1+x)^{1-n}\left[\left(\beta_{m,k}-1\right)(1+x)^{n+1}-(n+1)(1+x)^{n}\right],$$

and therefore vanishes for $n \geq 2$, as desired. □

We will exploit the above proposition extensively in Chapter 4. It should be noted that this process can be inverted; i.e. we can write the truncated hypergeometric series as sums of Atkin polynomials. However, we shall not need this fact in what follows.

To see how the second part of Theorem 3 follows from this proposition, notice that for any $0 \leq \ell \leq n$,

$$\begin{aligned} U^0_{n-\ell,m,k}(J) &= J^{n-\ell}\sum_{i=0}^{n-\ell}\frac{\left(\alpha_{m,k}\right)_i\left(\beta_{m,k}\right)_i}{i!^2 J^i} \\ &= \sum_{i=\ell}^{n}\binom{-\alpha_{m,k}}{i-\ell}\binom{-\beta_{m,k}}{i-\ell}J^{n-i}, \end{aligned}$$

under the transformation $i \to i+\ell$. Therefore, using the first equation in Proposition 15, we have

$$\begin{aligned} \mathcal{A}_{n,m,k}(J) &= \sum_{\ell=0}^{n}(-1)^{\ell}\binom{n+\alpha_{m,k}}{\ell}\binom{n+\beta_{m,k}-1}{\ell}\binom{2n-1}{\ell}^{-1}U^0_{n-\ell,m,k}(J) \\ &= \sum_{\ell=0}^{n}\sum_{i=\ell}^{n}(-1)^{\ell}\binom{n+\alpha_{m,k}}{\ell}\binom{n+\beta_{m,k}-1}{\ell}\binom{2n-1}{\ell}^{-1}\binom{-\alpha_{m,k}}{i-\ell}\binom{-\beta_{m,k}}{i-\ell}J^{n-i} \\ &= \sum_{i=0}^{n}J^{n-i}\left[\sum_{\ell=0}^{i}(-1)^{\ell}\binom{n+\alpha_{m,k}}{\ell}\binom{n-1+\beta_{m,k}}{\ell}\binom{2n-1}{\ell}^{-1}\binom{-\alpha_{m,k}}{i-\ell}\binom{-\beta_{m,k}}{i-\ell}\right], \end{aligned}$$

by interchanging the two sums. This last expression is precisely the one given in the theorem, so the proof is complete.

CHAPTER 3

The Family of Curves $\mathcal{F}_m$

Now that we have proven the existence of Atkin type polynomials $\mathcal{A}_{n,m,k}$, we would like to investigate their zeros in order to prove Theorem 4. As stated in the introduction, the zeros of these polynomials are closely related to properties of families of curves, denoted here by $\mathcal{F}_m$. It is not yet clear, however, why these particular families should arise. In this chapter, we explain how these curves emerge. This material is independent from what follows, so the reader interested only in the proof of Theorem 4 can skip to the next chapter.

We provide two explanations for the origins the family of curves $\mathcal{F}_m$: one coming from monodromy, and one coming from the fundamental domain $G_m \backslash \mathbb{H}$ viewed as a space of isomorphism classes of curves in $\mathcal{F}_m$.

3.1. Monodromy and hypergeometric functions

Fix an $m \geq 3$. One way to explain the presence of the curves in $\mathcal{F}_m$ is that the monodromy group associated to such a curve is precisely the Hecke triangle group G_m. However, there is some ambiguity in what is meant by this phrase, so it is important to explain this terminology precisely.

3.1.1. Contemporary treatment of the monodromy group. In the more recent literature (e.g. [81]), the Hecke triangle group G_m is described as the monodromy group of the hypergeometric differential equation (2.1.3) where $a = \alpha_m$, $b = \beta_m = 1/2 - \alpha_m$, and $c = 1$. As we have already discussed, such a differential equation has two linearly independent solutions, but the explicit representation of these solutions typically depends on whether one is in a neighborhood of 0, 1, or ∞. More precisely, near $w = 0$ one can take

$$\begin{aligned} y_1 &= {}_2F_1\left(\alpha_m, \beta_m; 1; w\right) \\ y_2 &= {}_2F_1\left(\alpha_m, \beta_m; 1; w\right) \log w + F_1\left(\alpha_m, \beta_m; w\right) \end{aligned}$$

as a system of independent solutions; near $z = 1$ one has the system

$$\begin{aligned} y_3 &= {}_2F_1\left(\alpha_m, \beta_m; \frac{1}{2}; 1 - w\right) \\ y_4 &= (1-w)^{1/2}\, {}_2F_1\left(1 - \alpha_m, 1 - \beta_m; \frac{3}{2}; 1 - w\right), \end{aligned}$$

and near ∞ one has the system

$$\begin{aligned} y_5 &= (-w)^{-\alpha_m} {}_2F_1\left(\alpha_m, \alpha_m; \alpha_m + 1 - \beta_m; \frac{1}{w}\right) \\ y_6 &= (-w)^{-\beta_m} {}_2F_1\left(\beta_m, \beta_m; \beta_m + 1 - \alpha_m; \frac{1}{w}\right). \end{aligned}$$

Relations between these systems were exploited in the proof of Proposition 14; specific examples can also be seen below.

In this setting, a monodromy of the hypergeometric differential equation means a transformation of these fundamental solutions as z moves in a positively oriented closed loop around 0, 1, or ∞. For example, as w winds around 0, we see that y_1 remains unchanged, while y_2 transforms into $y_2 + 2\pi i y_1$. In other words, in the basis of solutions $\{y_2, y_1\}$, a closed loop in a neighborhood around zero gives rise to the monodromy matrix

$$M_0 = \begin{pmatrix} 1 & 2\pi i \\ 0 & 1 \end{pmatrix}.$$

If we fix a basis of solutions, then each loop around one of the points $0, 1, \infty$ gives rise to a corresponding monodromy matrix M_0, M_1, M_∞. The eigenvalues of these matrices are $\{1, 1\}$, $\{1, -1\}$, and $\left\{e^{2\pi i \alpha_m}, e^{2\pi i \beta_m}\right\}$, respectively, and the monodromy matrices satisfy

$$M_0 M_1 M_\infty = I.$$

These monodromy matrices induce transformations on the variable z satisfying

$$\text{(3.1.1)} \qquad \frac{2\pi i z}{\lambda_m} = \Phi_m(J) = \frac{y_2}{y_1} + \log A_m,$$

where y_2 and y_1 are evaluated at $w = 1/J$. The matrix M_0, when viewed as a fractional linear transformation on ratios of solutions to the hypergeometric differential equation, maps $\Phi_m(J)$ to $\Phi_m(J) + 2\pi i$. Since $2\pi i z/\lambda_m = \Phi_m(J)$, the corresponding transformation on z is $z \mapsto z + \lambda_m$. In other words, the monodromy matrix M_0 corresponds to the translation T_m.

Similarly, we have

$$\begin{pmatrix} y_2 \\ y_1 \end{pmatrix} = B_m \begin{pmatrix} y_4 \\ y_3 \end{pmatrix},$$

where

$$B_m = \begin{pmatrix} \frac{\Gamma(1/2)}{\Gamma(\alpha_m)\Gamma(\beta_m)} \left\{\frac{2\pi}{\lambda_m} - \log A_m\right\} & \frac{\Gamma(-1/2)}{\Gamma(1-\alpha_m)\Gamma(1-\beta_m)} \left\{-\frac{2\pi}{\lambda_m} - \log A_m\right\} \\ \frac{\Gamma(1/2)}{\Gamma(\alpha_m)\Gamma(\beta_m)} & \frac{\Gamma(-1/2)}{\Gamma(1-\alpha_m)\Gamma(1-\beta_m)} \end{pmatrix},$$

(for this and other transformation matrices in more general settings, see [7]). Because y_3 is unchanged as w winds around a loop near 1, while y_4 transforms into $-y_4$, in the basis $\{y_2, y_1\}$ the monodromy matrix M_1 is given by

$$M_1 = B_m \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} B_m^{-1},$$

and so M_1 maps y_2/y_1 to

$$\frac{-\log A_m y_2/y_1 + (2\pi/\lambda_m + \log A_m)\,(2\pi/\lambda_m - \log A_m)}{y_2/y_1 + \log A_m}.$$

Once again, replacing y_2/y_1 by $2\pi i z/\lambda_m - \log A_m$, we conclude that the monodromy matrix M_1 corresponds to the mapping $z \mapsto -1/z$. In other words, M_1 corresponds to S. Since the monodromy group is generated by M_0 and M_1, it follows that this group, when viewed as a group of transformations of z, is precisely the Hecke triangle group G_m.

One can also interpret the effect of one of the monodromies by recalling that ${}_2F_1\,(a, b; c; w)$ satisfies

$$(3.1.2)\qquad {}_2F_1\,(a, b; c; w) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \frac{1}{\left(1 - e^{2\pi i b}\right)\left(1 - e^{2\pi i (c-b)}\right)} \int_{\gamma_{01}} x^{b-1}(1-x)^{c-b-1}(1-wx)^{-a}dx,$$

where γ_{01} is a Pochhammer cycle around 0 and 1 (see Figure 3.1.1). In fact, we can view the above integral as the integral of a differential form $\frac{dx}{y}$, where x and y satisfy the equation

$$(3.1.3)\qquad y^N = x^A\,(1-x)^B\,(1-wx)^C\,,$$

N is the least common denominator of a, b and c, and

$$\begin{aligned} A &= N(1-b) \\ B &= N(1+b-c) \\ C &= Na. \end{aligned}$$

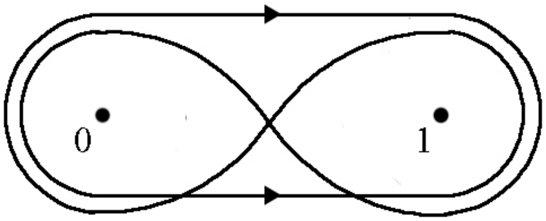

FIGURE 3.1.1. A Pochhammer cycle around 0 and 1

In this way, the hypergeometric functions can be viewed as period integrals on the Jacobian of the curve (3.1.3). In our present case, we see that

$$\begin{aligned} N &= \frac{4m}{(m-2,m+2)}, \\ A &= \frac{3m-2}{(m-2,m+2)}, \\ B &= \frac{m+2}{(m-2,m+2)}, \\ C &= \frac{m-2}{(m-2,m+2)}. \end{aligned}$$

From the perspective of period integrals, as w winds around one of the points $0, 1, \infty$, this has the effect of transforming the Pochhammer cycle. Integrating over a different path transforms the period, and therefore the monodromy group acts on ratios of periods. To put it another way, since $1/w$ is a branch point of the Riemann surface defined by (3.1.3), we are obtaining a monodromy group by rotating this branch point in a closed loop around other branch points.

This is the point of view emphasized in the older works of [30, 78], and particularly the work of Richard Morris in [53]. This series of papers appears to have been largely ignored, except for occasional references lamenting this very fact (see [9]). However, it is from the latter paper that one obtains the family of curves $\mathcal{F}_m$.

3.1.2. Morris's treatment of the monodromy group. The careful reader will observe that the curves given by (3.1.3) in the case $a = \alpha_m, b = \beta_m, c = 1$ are not the curves in the family $\mathcal{F}_m$ - in fact, they do not even have the correct genus (the genus of a curve given by (3.1.3) can be computed quite explicitly, see [2]). In contrast, Morris considers period integrals of the following general family of curves:

$$y^{\nu} = (x - r_1)^{\alpha} (x - r_2)^{\beta} (x - r_3)^{\gamma} (x - r_4)^{\delta} \tag{3.1.4}$$

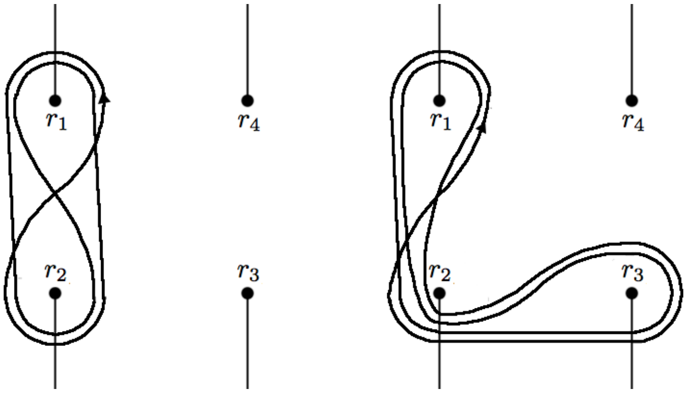

FIGURE 3.1.2. The contour a_1 (left) and its transformation when r_2 and r_3 are interchanged (right)

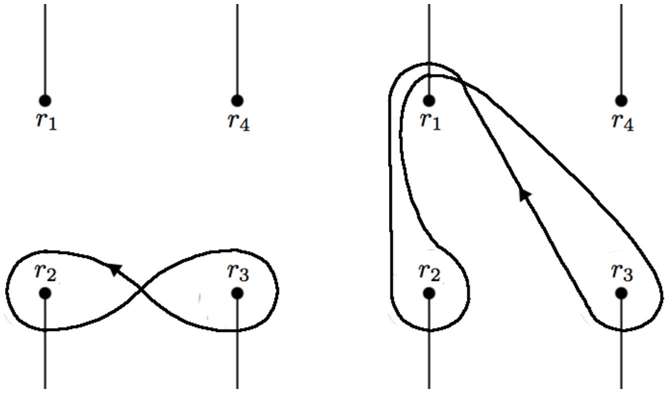

FIGURE 3.1.3. The contour b_1 (left) and its transformation when r_1 is rotated about r_2 positively (right)

where $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ satisfy $\alpha + \beta + \gamma + \delta = 2\nu$. In general this curve has four branch points, one at each r_i, and the period integrals he considers depend on how many of the exponents are equal. As it turns out, we need to consider the case when $\beta = \gamma = \nu/2$.

If one considers the Riemann surface associated to such a curve, one can again construct monodromies by rotating branch points around one another. The period integrals Morris considers are integrals of the differential form dx/y over the curves a_1 and b_1, pictured on the left in Figures 3.1.2 and 3.1.3, respectively. In each of these figures, the branch cuts are denoted by straight lines originating from each of the four branch points, and each time the one of the contours crosses one of these branches, it moves onto another sheet of the Riemann surface. Morris keeps careful track of how the contours depend on these sheets in his original paper.

When $\beta = \gamma$, the monodromy group is generated by two branch point transformations. The first transformation is the interchange of r_2 and r_3. The shape of the contour b_1 is unchanged by this transformation, though it is moved onto different sheets of the Riemann surface. The contour a_1 is transformed into the contour shown in Figure 3.1.2. The second is the rotation of r_1 about r_2 once in the positive direction. This first transformation does not change the shape of the contour a_1, though it does shift the contour onto different sheets; the transformation of b_1 is shown in Figure 3.1.3.

If we consider the differential form dx/y, denote the integral of this form over a_1 by A_1, and denote the integral of this form over b_1 by B_1, then Morris explicitly writes down how the ratio of periods $w = A_1/B_1$ transforms under these monodromies. The rotation of r_1 about r_2 corresponds to the transformation

$$w \mapsto \frac{-e^{-2\pi i\alpha/\nu}w}{w+1},$$

while the interchange of r_2 and r_3 corresponds to the transformation

$$w \mapsto w + e^{-2\pi i\alpha/\nu} - 1.$$

Note that because the exponents on r_2 and r_3 are the same, b_1 need not be a Pochhammer cycle - replacing the contour by a Pochhammer cycle simply alters the value of the period integral by a factor of 2.

If we set $\nu = \frac{2m}{(2,m)}$ and $\alpha = 2\alpha_m\nu$, (3.1.4) becomes

$$y^{2m/(2,m)} = (x-r_1)^{\frac{m-2}{(2,m)}}(x-r_2)^{\frac{m}{(2,m)}}(x-r_3)^{\frac{m}{(2,m)}}(x-r_4)^{\frac{m+2}{(2,m)}}. \tag{3.1.5}$$

Moreover, if we consider the complex variable τ, related to w by the transformation

$$w = -e^{\pi i/m}\tau + e^{2\pi i/m},$$

then the above transformations on τ become

$$\tau \mapsto \frac{1}{-\tau+\lambda_m} = ST_m^{-1}\tau,$$

and

$$\tau \mapsto \tau + \lambda_m = T_m\tau,$$

respectively. Therefore, these monodromies once again generate the Hecke triangle group G_m.

However, the curves given by (3.1.5) are not the same as the curves given by (3.1.3) with $a = \alpha_m$, $b = \beta_m$, $c = 1$. In fact, if we transform three of the branch points to $0, 1$, and ∞, say by setting

$$t = \frac{x-r_2}{x-r_4}\frac{r_3-r_4}{r_3-r_2},$$

then we can express A_1 and B_1 in terms of hypergeometric functions of the variable z, where

$$z = \frac{r_4 - r_1}{r_2 - r_1} \frac{r_2 - r_3}{r_4 - r_3} \tag{3.1.6}$$

is a cross ratio of the branch points (the details of this will be given in Section 3.2). In particular, B_1 essentially corresponds to a hypergeometric function in the variable z with $a = 2\alpha_m$, $b = 1/2$, $c = 1$. In the terminology of Section 3.1.1, these values of a, b, c still give rise to a certain triangle group for the monodromy group, but in this case we have

$$\begin{aligned} N &= \frac{2m}{(2,m)}, \\ A &= \frac{m}{(2,m)}, \\ B &= \frac{m}{(2,m)}, \\ C &= \frac{m-2}{(2,m)}, \end{aligned}$$

and the corresponding triangle group has signature (m, m, ∞), which is an index two subgroup of the Hecke triangle group G_m of signature $(2, m, \infty)$. How is it, then, that Morris obtains G_m as the monodromy group rather than an index two subgroup of this group?

3.1.3. Resolving the two treatments of the monodromy group.

The issue here is that the hypergeometric function described in the previous section is a function of a cross ratio of the branch points, while the hypergeometric functions in Section 3.1.1 are functions of the variable $J = J_m$. To understand how these two variables are related, we first show how we get from the family of curves (3.1.5) to the family of hyperelliptic curves $\mathcal{F}_m$. The idea is to find a suitable birational transformation between these two families. In fact, we prove a slightly more general statement.

Proposition 16. *Let $m > 3$ be a whole number, and let k be a fixed number coprime to m and less than $m/2$. Over an algebraically closed field, any curve of the form*

$$y^{2m/(2,m)} = (x - r_1)^{\frac{m-2k}{(2,m)}} (x - r_2)^{\frac{m}{(2,m)}} (x - r_3)^{\frac{m}{(2,m)}} (x - r_4)^{\frac{m+2k}{(2,m)}} \tag{3.1.7}$$

is birationally equivalent to a curve in $\mathcal{F}_m$.

Proof. To prove this result we need to find birational transformations between these curves in (x, y) coordinates and the curves defining $\mathcal{F}_m$, whose coordinates we will denote by (ξ, η) throughout so as to avoid confusion. In other words, we need ξ and η to satsify

$$\eta^2 = \xi^{2g+1+\kappa_m} - 2a\xi^{g+1} + b\xi^{1-\kappa_m}$$

for some parameters a and b, where g and κ_m are given in the introduction.

The idea, first, is for ξ to satisfy

$$\xi^{m/(2,m)} = \frac{x - r_1}{x - r_4}. \tag{3.1.8}$$

It's not clear yet that such a ξ can be given as a rational transformation of x and y. If such a ξ exists, however, then notice we can write

$$y^{2m/(2,m)} = \frac{\left[\left(x - r_1\right)\left(x - r_2\right)\left(x - r_3\right)\left(x - r_4\right)\right]^{\frac{m}{(2,m)}}}{\xi^{2km/(2,m)^2}}.$$

If we take a formal $m/(2,m)^{th}$ root of the above expression, we get another relation between ξ, x, and y. In particular, if we want ξ to satisfy (3.1.8) along with

$$\xi^{2k/(2,m)} = \frac{\left(x - r_1\right)\left(x - r_2\right)\left(x - r_3\right)\left(x - r_4\right)}{y^2},$$

then this determines ξ uniquely as a rational function of x and y, since $m/(2,m)$ and $2k/(2,m)$ are coprime. We may therefore conclude that ξ is a rational function of x and y, and consequently x is a rational function of ξ, since (3.1.8) implies that

$$x = \frac{r_4\xi^{m/(2,m)} - r_1}{\xi^{m/(2,m)} - 1}. \tag{3.1.9}$$

Next, we define η_0 by

$$\eta_0 = \frac{y\left(r_1 - r_4\right)}{\xi^c \left(x - r_4\right)^2}$$

where

$$c = \frac{1}{2}\left(g - \frac{2k}{(2,m)} + 2\kappa_m - 1\right) \in \mathbb{Z}.$$

Since ξ can be written as a rational function of x and y, so can η_0. Moreover, using (3.1.9) we see that y can be written as a rational function of ξ and η_0. Therefore, the change of variables from (x, y) to (ξ, η_0) really does represent a birational transformation.

Given our choice of ξ, we have

$$\begin{aligned} \eta_0^2 &= \frac{y^2\left(r_1 - r_4\right)^2}{\xi^{2c}\left(x - r_4\right)^4} \\ &= \xi^{1-\kappa_m}\frac{\left(x - r_2\right)\left(x - r_3\right)\left(r_1 - r_4\right)^2}{\left(x - r_4\right)^2}, \end{aligned}$$

by our choice of c. Again using (3.1.9), it follows that

$$\frac{(x-r_2)(x-r_3)(r_1-r_4)^2}{(x-r_4)^2} = (r_4-r_2)(r_4-r_3)\left(\xi^{2m/(2,m)} - 2a\xi^{m/(2,m)} + b\right),$$

where

$$\begin{aligned} a &= \frac{1}{2}\left(\frac{r_1-r_2}{r_4-r_2} + \frac{r_1-r_3}{r_4-r_3}\right) \\ b &= \left(\frac{r_1-r_2}{r_4-r_2}\right)\left(\frac{r_1-r_3}{r_4-r_3}\right). \end{aligned}$$

Upon setting $\eta = \frac{\eta_0}{[(r_4-r_2)(r_4-r_3)]^{1/2}}$, we obtain

$$\begin{aligned} \eta^2 &= \xi^{1-\kappa_m}\left(\xi^{2m/(2,m)} - 2a\xi^{m/(2,m)} + b\right) \\ &= \xi^{2g+1+\kappa_m} - 2a\xi^{g+1} + b\xi^{1-\kappa_m}, \end{aligned}$$

by definition of g. □

Remark. The reason for considering an arbitrary k coprime to m and less than $m/2$ in the above statement, rather than simply the case $k=1$, is because the monodromy groups for curves for general k correspond to the non-discrete groups $G_{m,k}$ (i.e. the Galois conjugates of G_m) corresponding to the hyperbolic triangle with angles $\left(0, \frac{\pi k}{m}, \frac{\pi}{2}\right)$ at the vertices. As these triangles and groups have already appeared in previous chapters, it is instructive to investigate the corresponding curves as well.

We can use the above proposition to understand the relationship between the cross ratio z given by (3.1.6) and the variable J, defined in terms of the family of curves $\mathcal{F}_m$ as the ratio $\frac{b}{b-a^2}$. Writing a, b, and z in terms of the branch points r_i and solving for J in terms of z gives the identity

$$J = \frac{4(z-1)}{z^2}. \tag{3.1.10}$$

Let us now compare the monodromies discussed in the previous sections. From Section 3.1.1, we know that when J winds around 0 once in the positive direction, we obtain the monodromy matrix $M_\infty = ST_m^{-1}$. On the other hand, if we consider the mapping

$$t = \frac{x-r_2}{x-r_4}\frac{r_3-r_4}{r_3-r_2}, \tag{3.1.11}$$

where the r_i denote the branch points of the curve (3.1.5), we see that $r_2 \mapsto 0$ and $r_1 \mapsto 1/z$, so that the winding of r_1 about r_2 in the positive direction corresponds to the winding of $1/z$ about 0 in the positive direction. We saw in Section 3.1.2 that this monodromy corresponds to ST_m^{-1} as well. Also, by (3.1.10), for

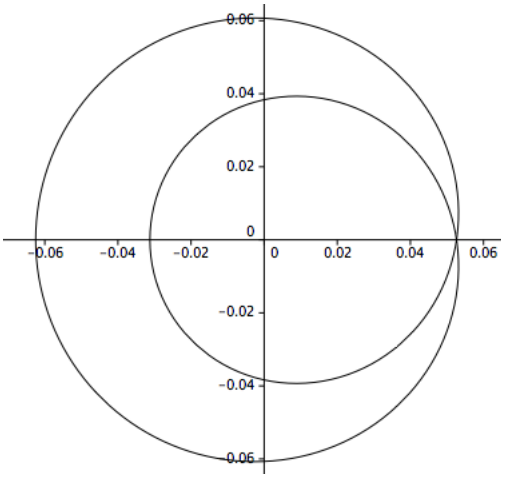

FIGURE 3.1.4. The transformation of $z = \frac{e^{i\theta}}{2}, 0 \leq \theta < 2\pi$, under the mapping J

$1/z$ sufficiently close to 0, this monodromy results in a winding of J about 0 once in the positive direction. So it comes as no surprise that these give rise to the same matrix.

Next, consider what happens when $1/J$ winds around 0 once in the positive direction. This corresponds to the monodromy matrix M_0 given by the translation T_m. On the other hand, if we consider the mapping

$$t = \frac{x - r_2}{x - r_4} \frac{r_1 - r_4}{r_1 - r_2}, \tag{3.1.12}$$

we see this time that $r_2 \mapsto 0$ while $r_3 \mapsto z$, so that the interchange of r_2 and r_3 is equivalent to z winding halfway around 0 in the positive direction. We know from above that this monodromy also corresponds to the translation matrix T_m. On the other hand, this is not a monodromy of the cross ratio z in the traditional sense, since z does not wind around a closed loop. If we wind z around 0 so that it ends up in its starting position, this is the same as applying the translation matrix twice.

Comparing this to what happens with J, we see that when z winds around 0 once in the positive direction, $1/J$ winds around 0 *twice* in the positive direction (see Figure 3.1.4). Therefore, we see that these different families of curves are giving rise to the same "monodromy" groups because in the case of Morris, one of the monodromies is really only half of a monodromy. If we let z make a full revolution around 0, the corresponding group is indeed an index 2 subgroup of the Hecke group G_m.

Note that the relationship between z and J also becomes apparent through certain quadratic transformation formulas for hypergeometric functions. For example, it is well known that

$$_2F_1\left(a, b; 2b; z\right) = (1-z)^{-a/2}\, {_2F_1}\left(\frac{a}{2}, b - \frac{a}{2}; b + \frac{1}{2}; \frac{z^2}{4(z-1)}\right)$$

when $|\arg(1-z)| < \pi$. Another example is

$$ {}_2F_1(a, 1-a; c; z) = (1-z)^{c-1} \, {}_2F_1\left(\frac{c-a}{2}, \frac{c+a-1}{2}; c; 4z(1-z)\right), $$

valid when the real part of z is less than 1.

Such quadratic transformation laws can be used to relate the period integrals encountered in Section 3.1.1 to the period integrals encountered in Section 3.1.2. For example, when $a = 2\alpha_m, b = 1/2$, the first formula above becomes

$$ {}_2F_1\left(2\alpha_m, \frac{1}{2}; 1; z\right) = (1-z)^{-\alpha_m} \, {}_2F_1\left(\alpha_m, \beta_m; 1; \frac{1}{J}\right). \tag{3.1.13} $$

Similarly, when $a = \frac{1}{2}$, $c = \frac{3}{2} - 2\alpha_m$, the second formula evaluated at $1/z$ becomes

$$ {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; \frac{3}{2} - 2\alpha_m; \frac{1}{z}\right) = (1-z)^{1/2-2\alpha_m} \, {}_2F_1\left(\frac{1}{2} - \alpha_m, \frac{1}{2} - \alpha_m; \frac{3}{2} - 2\alpha_m; J\right). \tag{3.1.14} $$

We will apply these formulas in the next section.

3.2. Resolving definitions of J_m and exploring moduli spaces

We now turn towards a connection between points in $G_m \backslash \mathbb{H}$ and isomorphism classes of curves in $\mathcal{F}_m$. Before embarking on such a discussion, though, we need to resolve the two different definitions of J that have been presented thus far.

3.2.1. Two definitions of the J function. We have presented two definitions of J_m. One of them is analytic, and gives J_m as a ratio of modular forms for the Hecke triangle group G_m (see equation (2.1.10)). The other definition is algebraic, and is defined by the nonzero coefficients on the right hand side of an equation defining a curve in $\mathcal{F}_m$ (see the statement of Theorem 4). In this section we will see how these two definitions coincide. This will allow us to prove a result on isomorphism classes of hyperelliptic curves and the space $G_m \backslash \mathbb{H}$, which does not appear to be present in the literature.

To make the connection between the analytic and algebraic definitions of J_m, we need to show that for a curve

$$ y^2 = x^{1-\kappa_m}\left(x^{2g+2\kappa_m} - 2ax^{g+\kappa_m} + b\right) $$

in $\mathcal{F}_m$, we can associate a value $\tau \in \mathbb{H}$ such that

$$ \frac{b}{b-a^2} = J = J_m(\tau) = \frac{f_0^m(\tau)}{f_0^m(\tau) - f_i^2(\tau)}, $$

where, again, f_0 and f_i represent the canonical modular forms on G_m. Such a connection is made possible by the work in the sections above.

Throughout the remainder of this section, fix the same notation as in Section 3.1.2. If we begin with a curve of the form (3.1.5), the key is to relate the cross ratio z to a value τ in the upper half plane. This can be done with some careful calculation related to the ratio of period integrals A_1/B_1. First, note that the value of the period B_1 is defined by

$$B_1 = \int_{b_1} \frac{dx}{y}.$$

In this case, without loss of generality we assume that

$$\begin{aligned} r_1 &= 1/z, \\ r_2 &= 0, \\ r_3 &= 1, \\ r_4 &= \infty \end{aligned}$$

for some complex number z. We can reduce to such a case by means of the mapping (3.1.11) which sends r_1 to $1/z$ where z is the cross ratio (3.1.6), though one needs to be more careful about the branching behavior of the relevant complex roots. In any event, given this assumption, we see

$$\int_{b_1} \frac{dx}{y} = \int_{b_1} \frac{dx}{\left(x - \frac{1}{z}\right)^{2\alpha_m} x^{1/2} \left(x-1\right)^{1/2}},$$

where b_1 is as in Figure 3.1.3. In fact, because $A/N = B/N = 1/2$, the value of this integral is one half of the integral over the Pochhammer cycle around 0 and 1. When combined with (3.1.2) and (3.1.13) we obtain, for say $\mathrm{Re}z < 1/2$,

$$\begin{aligned} B_1 &= \frac{2\pi}{i\left(-1/z\right)^{2\alpha_m}} {}_2F_1\left(2\alpha_m, \frac{1}{2}; 1; z\right) \\ &= \frac{2\pi}{i\left(-1/z\right)^{2\alpha_m}} {}_2F_1\left(\alpha_m, \beta_m; 1; \frac{1}{J}\right). \end{aligned}$$

In terms of the six solutions to the hypergeometric differential equation given at the beginning of Section 3.1.1, we have

$$B_1 = \frac{2\pi}{i\left(-1/z\right)^{2\alpha_m}} (1-z)^{-\alpha_m} y_1(1/J),$$

where J is defined in terms of the cross ratio z by (3.1.10).

We can perform an analogous calculation with A_1. In this case, a_1 is a Pochhammer loop around 0 and $1/z$, so by making the change of variables

$$t = zx,$$

we transform a_1 to $t\left(a_1\right)$, a Pochhammer cycle around 0 and 1. By (3.1.2) and (3.1.14), A_1 then becomes

$$\begin{aligned} A_1 = \int_{a_1} \frac{dx}{y} &= \frac{1}{iz^{1/2}(-1/z)^{2\alpha_m}} \int_{t(a_1)} \frac{dt}{t^{1/2}\,(1-t)^{2\alpha_m}\,\left(1-\frac{t}{z}\right)^{1/2}} \\ &= \frac{2e^{\pi i/m}\lambda_m}{iz^{1/2}(-1/z)^{2\alpha_m}} \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(1-2\alpha_m\right)}{\Gamma\left(\frac{3}{2}-2\alpha_m\right)} {}_2F_1\left(\frac{1}{2},\frac{1}{2};\frac{3}{2}-2\alpha_m;z\right) \\ &= \frac{2e^{\pi i/m}\lambda_m}{iz^{1/2}(-1/z)^{2\alpha_m}} \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(1-2\alpha_m\right)}{\Gamma\left(\frac{3}{2}-2\alpha_m\right)} \left(\frac{1-z}{-z}\right)^{\frac{1}{2}-2\alpha_m} \left(\frac{(-z)^2}{4\,(1-z)}\right)^{\beta} y_6(1/J). \end{aligned}$$

where y_6 is as given in beginning of Section (3.1.1).

If we now calculate the quotient A_1/B_1, many of the terms depending on z cancel, and since $\alpha_m + \beta_m = 1/2$ we find

$$\begin{aligned} \frac{A_1}{B_1} &= \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(1-2\alpha_m\right)}{4^{\beta_m} i\Gamma\left(\frac{3}{2}-2\alpha_m\right)} \lambda_m e^{\pi i/m} \frac{y_6(1/J)}{y_1(1/J)} \\ &= \frac{\lambda_m e^{\pi i/m}}{2\pi i} \frac{\Gamma\left(\beta_m\right)\Gamma\left(1-\alpha_m\right)}{\Gamma\left(\beta_m+1-\alpha_m\right)} \frac{y_6(1/J)}{y_1(1/J)}, \end{aligned} \tag{3.2.1}$$

because of the standard transformation law for the Gamma function

$$\Gamma\left(1-\alpha_m\right)\Gamma\left(\frac{1}{2}-\alpha_m\right) = \sqrt{\pi}2^{2\alpha_m}\Gamma\left(1-2\alpha_m\right).$$

We now have an expression for A_1/B_1 in terms of the algebraic definition of J. On the other hand, we have previously defined

$$A_1/B_1 = -e^{\pi i/m}\tau + e^{2\pi i/m},$$

where monodromies of the branch points of the curve are equivalent to actions of G_m on τ. In particular, for τ in the fundamental domain of $G_m\backslash\mathbb{H}$, by the analytic definition of $J_m(\tau)$ we have

$$\begin{aligned} \frac{2\pi i\tau}{\lambda_m} &= \Phi_m\left(J_m(\tau)\right) \\ &= \frac{y_2\left(1/J_m(\tau)\right)}{y_1\left(1/J_m(\tau)\right)} + \log A_m, \end{aligned}$$

by (3.1.1). Combining this with (3.2.1), we find that the algebraic value J and the analytic function $J_m(\tau)$ are related via the equation

$$\frac{2\pi i e^{\pi i/m}}{\lambda_m} - \frac{\Gamma\left(\beta_m\right)\Gamma\left(1-\alpha_m\right)}{\Gamma\left(\beta_m+1-\alpha_m\right)} \frac{y_6(1/J)}{y_1(1/J)} = \Phi_m\left(J_m(\tau)\right).$$

Next, by the formulas in section 395 [7], we see that y_6 is related to y_1 and y_2 via the equation

$$y_6 = \frac{\Gamma\left(\beta_m+1-\alpha_m\right)}{\Gamma\left(\beta_m\right)\Gamma\left(1-\alpha_m\right)}\left[\left(C_m+\pi i\right)y_1 - y_2\right],$$

where

$$\begin{aligned} C_m &= 2\frac{\Gamma'}{\Gamma}(1) - \frac{\Gamma'}{\Gamma}(\beta_m) - \frac{\Gamma'}{\Gamma}(1-\alpha_m) \\ &= -\log A_m + \frac{\Gamma'}{\Gamma}(1-\beta_m) - \frac{\Gamma'}{\Gamma}(\beta_m) - \pi\sec(\pi(\beta_m - \alpha_m)) \\ &= -\log A_m + \pi\cot(\pi\beta_m) - \pi\sec\left(\pi\left(2\beta_m - \frac{1}{2}\right)\right) \\ &= -\log A_m + \pi\cot(2\pi\beta_m), \end{aligned}$$

where we have applied (2.2.10) in the third line.

Writing C_m in terms of A_m and using trigonometry we find

$$\begin{aligned} \Phi_m(J_m(\tau)) &= \frac{2\pi i e^{\pi i/m}}{\lambda_m} - \pi\cot(2\pi\beta_m) - \pi i + \Phi_m(J) \\ &= \Phi_m(J). \end{aligned}$$

Taking inverses yields

$$\begin{aligned} \tau &= \frac{\lambda_m}{2\pi i}\Phi_m(J) \\ &= \frac{\lambda_m}{2\pi i}\Phi_m\left(\frac{4(z-1)}{z^2}\right) \\ &= \frac{\lambda_m}{2\pi i}\Phi_m\left(\frac{b}{b-a^2}\right), \end{aligned}$$

and so by applying J_m to both sides we obtain

$$J_m(\tau) = \frac{b}{b-a^2} = J,$$

as desired.

Note that these calculations can be interpreted within the framework of the Thomae formula, which can be used to related periods of hyperelliptic integrals in terms of certain $\theta-$constants to the branch points of the curve. For more on this topic, see Thomae's original treatment [74], as well as more recent discussions in [19, 43, 70].

3.2.2. Isomorphism classes of curves in $\mathcal{F}_m$. We now prove a result on the isomorphism classes of curves in $\mathcal{F}_m$, analogous to the statement relating isomorphism classes of elliptic curves to points in the fundamental domain for $G_3\backslash\mathbb{H}$. Our main result, which does not seem to appear anywhere in the literature, associates to any τ in the fundamental domain of $G_m\backslash\mathbb{H}$ an isomorphism class of hyperelliptic curves in $\mathcal{F}_m$.

We first record the following proposition which gives us an easy way to check whether or not two hyperelliptic curves are isomoprhic. The interested reader can consult [49, 50] for more details.

Proposition 17. *Let C_1 and C_2 be two hyperelliptic curves of genus g over $\mathbb{C}$ with affine equations*

$$C_i: \ y^2 = f_i(x)$$

where both of the polynomials f_i have simple roots. Then any isomorphism between these curves is of the form

$$(x,y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}}\right) \tag{3.2.2}$$

for some $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ and some $e \in \mathbb{C}\backslash\{0\}$. Such an isomorphism is determined uniquely by the class of pairs

$$\left(wM, w^{g+1}e\right) \tag{3.2.3}$$

for $z \in \mathbb{C}\backslash\{0\}$.

We will rely on this proposition to prove the following theorem.

Theorem 18. *The points $\tau \in \mathbb{H}$ correspond to isomorphism classes of hyperelliptic curves in $\mathcal{F}_m$ via the mapping*

$$\tau \mapsto \{C_\tau\}$$

where where $\{C_\tau\}$ denotes the isomorphism class of hyperelliptic curves containing the specific curve

$$C_\tau: \ y^2 = x^{1-\kappa_m}\left(x^{2m/(2,m)} - 2f_i(\tau)x^{m/(2,m)} + f_0(\tau)^m\right).$$

Here f_0 and f_i are the canonical modular forms for $G_m\backslash\mathbb{H}$ defined in Chapter 2. Moreover, two curves in $\mathcal{F}_m$ are isomorphic if and only if their corresponding J values are equal, and therefore the above mapping gives a bijection between points τ in $G_m\backslash\mathbb{H}$ and isomorphism classes of hyperelliptic curves with invariant $J_m(\tau)$.

One direction in the proof of this theorem is fairly straightforward. Namely, suppose we have two curves in $\mathcal{F}_m$ of the form

$$\begin{aligned} C_1 : \; y^2 &= x^{1-\kappa_m}\left(x^{2m/(2,m)} - 2a_1 x^{m/(2,m)} + b_1\right) \\ C_2 : \; y^2 &= x^{1-\kappa_m}\left(x^{2m/(2,m)} - 2a_2 x^{m/(2,m)} + b_2\right) \end{aligned}$$

with equal J invariants, i.e.

$$\frac{b_1}{b_1 - a_1^2} = \frac{b_2}{b_2 - a_2^2}.$$

From the previous section, we have seen there exists a $\tau \in \mathbb{H}$ so that

$$\frac{b_j}{b_j - a_j^2} = \frac{f_0^m(\tau)}{f_0^m(\tau) - f_i^2(\tau)}$$

for $j = 1, 2$. Without loss of generality we may assume $b_j \neq 0$, since otherwise the polynomial defining the curve does not have simple roots. One can slightly modify the argument as in the proof of Theorem 4 in the case $b_j = 0$. We also continue to assume that $b_j \neq a_j^2$.

Based on these assumptions, the above equality implies that

$$b_j = \frac{f_0^m(\tau)}{f_i^2(\tau)} a_j^2.$$

Therefore, if we define an isomorphism $\phi_j = (M_j, e_j)$, where

$$\begin{aligned} M_j &= \begin{pmatrix} a_j^{(2,m)/m} & 0 \\ 0 & f_i^{(2,m)/m}(\tau) \end{pmatrix}, \\ e_j &= a_j^{1+\frac{(2,m)}{2m}(1-\kappa_m)} f_i^{\frac{(2,m)}{2m}(1-\kappa_m)}(\tau), \end{aligned}$$

then ϕ_j is an isomorphism between C_j and the curve C_τ. Thus, the curves are isomorphic via the isomorphism $\phi = \phi_2^{-1}\phi_1$.

The other direction is a bit more complicated. Suppose we have two curves C_1 and C_2 in $\mathcal{F}_m$ which are isomorphic. Again, we assume their J invariants are nonzero; if one invariant is zero and one is nonzero, the curves have different genus and are therefore not isomorphic, while if both are zero there is nothing to show. Given that the J invariants are nonzero, we must show they are equal.

First, note that any isomorphism of hyperelliptic curves is equivalent to an action on the roots of the polynomial defining the curve under the action of some Möbius transformation. More specifically, given any isomorphism of the form (3.2.2), direct computation shows that the equation of the curve

$$y^2 = \prod_{i=1}^{2g+1+\epsilon} (x - \alpha_i)$$

transforms to

$$e^2 y^2 = c^{1-\epsilon} \prod_{i=1}^{2g+1+\epsilon} (a - \alpha_i c) \left[\left(x - M^{-1}\infty\right)^{1-\epsilon} \prod_{i=1}^{2g+1+\epsilon} \left(x - M^{-1}\alpha_i\right) \right].$$

Here $\epsilon = 0$ or 1 according to the degree of f. By choosing w appropriately in (3.2.3), we can therefore assume that the isomorphism transforms the equation of the curve to one of the form

$$y^2 = \left(x - M^{-1}\infty\right)^{1-\epsilon} \prod_{i=1}^{2g+1+\epsilon} \left(x - M^{-1}\alpha_i\right).$$

In other words, M as a Möbius transformation maps roots of C_2 to roots of C_1.

In the case of the family of curves in $\mathcal{F}_m$, we may apply a birational transformation to convert each C_j to a curve with equation of the form

$$y^2 = x^{1-\kappa_m} \left(x^{m/(2,m)} - 1\right) \left(x^{m/(2,m)} - \sigma_j\right)$$

where each $\sigma_j \neq 0, 1$ is related to $J_j = \frac{b_j}{b_j - a_j^2}$ via

$$J_j = \frac{-4\sigma_j}{\left(1 - \sigma_j\right)^2}.$$

We will show that $J_1 = J_2$ if C_1 and C_2 are isomorphic in the case $m \equiv 2 \bmod 4$; the other cases can be proven similarly.

When $m \equiv 2 \bmod 4$, the equations of the curves C_j reduce to

$$y^2 = \left(x^{m/2} - 1\right) \left(x^{m/2} - \sigma_j\right).$$

If we let ω_j be a root of the equation $\omega_j^{m/2} = \sigma_j$, and let $\zeta = \zeta_{m/2} = e^{4\pi i/m}$, then the roots of the polynomial on the right hand side are of the form $\zeta^k \omega_j^\delta$ for $1 \leq k \leq m/2$ and $0 \leq \delta \leq 1$. Suppose an isomorphism between these two curves exists. Our argument splits into two cases, depending on the size of the genus of the curves.

If $g \geq 4$, then since $g = m/2 - 1$ in the case under consideration, we see that the polynomial on the right hand side of the equation defining C_j has at least ten roots. Of these roots, half are on the unit circle, and half are on the circle $\{z : |z| = |w_j|\}$. Because the number of roots on each circle is at least five, and because a circle can intersect a pair of concentric circles in at most four points, this means the pair of circles $\{z : |z| = 1\}$ and $\{z : |z| = |w_2|\}$ is mapped to the pair of circles $\{z : |z| = 1\}$ and $\{z : |z| = |w_1|\}$. This is true because otherwise, at least one of the roots on one of the first pair of circles could not all intersect the second pair of circles, which is a contradiction because we have assumed the existence of an isomorphism. In fact, if we replace M by

$$\begin{pmatrix} 1/w_1 & 0 \\ 0 & 1 \end{pmatrix}^{\epsilon} M$$

for $\epsilon \in \{0, 1\}$ as necessary, we may assume our Möbius transformation sends the unit circle to itself and the circle of radius $r_2 = |w_2|$ to the circle of radius $r_1 = |w_1|^{(-1)^{\epsilon}}$. Proving the result for such a modified M then gives the result for the original isomorphism.

We now recall some standard facts about Möbius transformations. First, it is well known that any Möbius transformation mapping the unit circle to itself can be written in the form

$$\begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix},$$

for some complex numbers α and β. This can be seen by mapping the unit circle to the real axis and classifying all Möbius transformations which preserve the real axis. It is also known (see for example [23]) that any Möbius transformation mapping a pair of concentric circles to a pair of concentric circles preserves the ratio of the radii of the circles.

Combining these facts with the observations from the previous paragraph, without loss of generality there exist complex numbers α and β such that for for any θ, our Möbius transformation satisfies

$$\left|\frac{\alpha r_2 e^{i\theta} + \beta}{\overline{\beta} r_2 e^{i\theta} + \overline{\alpha}}\right| = r_1,$$

where $r_1 = r_2$ or $r_1 = 1/r_2$. This is equivalent to the statement that

$$2r_2\left(r_1^2 - 1\right)\operatorname{Re}\left(\alpha\overline{\beta}e^{i\theta}\right) = |\alpha|^2\left(r_2^2 - r_1^2\right) + |\beta|^2\left(1 - (r_1 r_2)^2\right).$$

If $r_1 = r_2$, the first term on the right hand side fanishes, and the equation reduces to

$$\left(1 + r_1^2\right)|\beta|^2 + 2r_1\mathrm{Re}\left(\alpha\overline{\beta}e^{i\theta}\right) = 0,$$

which implies $\beta = 0$ since the first term is always positive and θ can be chosen arbitrarily. Similarly, if $r_1 = 1/r_2$ it follows that $\alpha = 0$. Hence, because we know M maps roots of C_2 to roots of C_1, it follows that either M is either a rotation or the composition of a rotation and an involution. Therefore either $\sigma_1 = \sigma_2$ or $\sigma_1 = \sigma_2^{-1}$; in either case, $J_1 = J_2$, as desired.

If $g < 4$, then $g = 2$ (equivalently $m = 6$). In this case the polynomials defining each curve have only six roots, three each on two concentric circles. In this case our argument from above may fail, because there are insufficiently many roots on each circle.

Consider the Möbius transformation $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ from the roots of C_2 to the roots of C_1. If M maps the pair of concentric circles formed by the roots of C_2 to the pair of concentric circles formed by the roots of C_1, then our previous argument applies. Otherwise, M maps exactly two roots on the unit circle to two roots on the unit circle or exactly one root on the unit circle to one root on the unit circle. By replacing M by

$$\begin{pmatrix} 1/w_1 & 0 \\ 0 & 1 \end{pmatrix}^{\epsilon} M \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}^{k} \begin{pmatrix} 0 & w_2 \\ 1 & 0 \end{pmatrix}^{\delta}$$

and w_1 by $w_1^{(-1)^\epsilon}$ as necessary for some $k \in \{0, 1, 2\}$ and some $\delta, \epsilon \in \{0, 1\}$, we may assume without loss of generality that M maps exactly two roots on the unit circle to two roots on the unit circle, and moreover $M(1) = 1$. We therefore need only consider the four cases $M(\zeta) = \zeta$, $M(\zeta) = \zeta^2$, $M\left(\zeta^2\right) = \zeta$, $M\left(\zeta^2\right) = \zeta^2$.

In the first case, $M(1) = 1$ and $M(\zeta) = \zeta$ implies that

$$\begin{aligned} a + b &= c + d, \\ a\zeta + b &= c\zeta^2 + d\zeta; \end{aligned}$$

solving for a and b in terms of c and d gives

$$M = \begin{pmatrix} d - c\zeta^2 & -c\zeta \\ c & d \end{pmatrix}.$$

If $c = 0$, M acts as the identity which is a contradiction, since we have assumed the existence of a point on the unit circle which is not mapped to the unit circle by M. Therefore we may assume c is nonzero and we can replace M by

$$M = \begin{pmatrix} u - \zeta^2 & -\zeta \\ 1 & u \end{pmatrix}$$

for the complex number $u = d/c$.

Renaming w_2 by ζw_2 or $\zeta^2 w_2$ as necessary, we may assume that $M(w_2) = \zeta^2$ for convenience, or equivalently $w_2 = \frac{\zeta^2 u + \zeta}{u - 2\zeta^2}$. Therefore, the images of $M\left(\zeta^2\right)$, $M(\zeta w_2)$ and $M\left(\zeta^2 w_2\right)$ must correspond to w_1,

ζw_1, and $\zeta^2 w_1$, respectively. In particular, this means

$$\begin{aligned}\frac{M\left(\zeta w_2\right)}{M\left(\zeta^2 w_2\right)} &= \zeta^j, \\ \frac{M\left(\zeta^2\right)}{M\left(\zeta^2 w_2\right)} &= \zeta^{-j},\end{aligned}$$

for some $j \in \{1,2\}$. Writing these equations in terms of u gives us two polynomials, which have no common root unless $j=2$. In this case, we have solutions when $u = \frac{\zeta^2}{2}\left(1 \pm \sqrt{3}\right)$, but in these cases one still obtains $\sigma_1 = 1/\sigma_2$ so that the J invariants are equal.

Finally, replacing M by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^m M \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n$$

for some $\{m,n\} \in \{0,1\} \times \{0,1\}$ allows us to apply the same argument to the other three cases mentioned above. So in any case, an isomorphism of curves in $\mathcal{F}_6$ implies the J invariants of the curves are equal, as was to be shown.

CHAPTER 4

Zeros of Generalized Atkin Polynomials

We now turn our attention to the zeros of generalized Atkin polynomials modulo primes. We will prove the result in full generality, though things simplify somewhat in the arithmetic cases $m = 3, 4, 6, \infty$. As we will see, the roots of Atkin-type polynomials in the general setting no longer detect supersingularity. Instead, they detect whether or not a curve is ordinary. In order to fully understand the statement of Theorem 4, we begin with some preliminary information.

4.1. Supersingularity and the Hasse-Witt matrix of a hyperelliptic curve

4.1.1. Supersingularity in general. Let us first recall what it means for a curve to be supersingular over a field of characteristic p, since this will turn out to be the condition detected by the Atkin polynomials in the arithmetic cases $m = 3, 4, 6, \infty$. In the case of an elliptic curve there are several equivalent definitions, all of them summarized by the following theorem (see, for example, [21] or [68]):

THEOREM 19. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ where $q = p^n$, p prime. Write the characteristic polynomial of the Frobenius endomorphism π (i.e. the endomorphism induced on the curve by the endomorphism $x \to x^q$ of $\mathbb{F}_q$) as $P(X) = X^2 - a_pX + q$, or, equivalently, write $\#E(\mathbb{F}_q) = q + 1 - a_p$. Then the following conditions are equivalent:*

(i) The endomorphism ring of E over $\overline{\mathbb{F}}_q$ is an order in a quaternion algebra.

(ii) E has no points of order p.

(iii) $a_p \equiv 0$ mod p.

(iv) There exists an integer k such that $\pi^k = \pm q^{k/2}$.

If any of the above conditions hold, E is said to be supersingular.

One can show that the number of supersingular polynomials modulo a fixed prime p is finite, and one can therefore construct, for any such p, a polynomial

$$ss_p(J) := \prod_{\substack{E/\overline{\mathbb{F}}_p \\ E \text{ supersingular}}} (J - J(E)) \in \mathbb{F}_p[j]$$

whose zeros are precisely the J invariants of supersingular elliptic curves. As it turns out, the coefficients of this polynomial lie in $\mathbb{F}_p$, and Atkin proved that the supersingular polynomial is congruent to $\mathcal{A}_{n_p}(J) = \mathcal{A}_{n_p,3,1}(J) \bmod p$, where $n_p = \deg ss_p(J)$. See Theorem 2 for the precise statement.

A proof of this theorem can be found in [40]. Note that J is a more natural parameter to consider than $j = 1728J$, since in general A_m will be transcendental. In particular, if we define monic orthogonal polynomials in terms of the variable $j_m = J_m/A_m$, the value A_m will appear in the recurrence relations and the closed formula for the Atkin polynomials, making it difficult to consider the reduction of these polynomials mod p in the nonarithmetic cases. By considering J_m, the generalized Atkin polynomials do not depend on A_m, so the reduction of these polynomials mod p proceeds smoothly.

In the cases $m = 4, 6$, the curves in $\mathcal{F}_m$ are no longer elliptic, and so we need a more general notion of supersingularity in order to discuss these cases. Such a generalization is provided for us in [57]:

Definition. Let A be an abelian variety defined over a finite field $\mathbb{F}_q$. A is called *supersingular* if A is isogenous over $\overline{\mathbb{F}}_q$ to a product of supersingular elliptic curves. Similarly, a curve C defined over $\mathbb{F}_q$ is said to be supersingular if the Jacobian of C is supersingular.

It is shown in [57] that this definition can be strengthened without loss of generality; in fact, the relevant isogeny can be defined over a finite extension of $\mathbb{F}_q$, and moreover, since all supersingular elliptic curves are isogenous, one can assume that a supersingular curve C has Jacobian isogenous to E^g, where E is a single supersingular elliptic curve, and g is the genus of C.

To further motivate this definition of supersingularity, consider the following analogue of Theorem 19 (see [21] for more details).

Theorem 20. *The following conditions for an abelian variety A over $\mathbb{F}_q$ of genus g are equivalent:*

(i) A is supersingular.

(ii) For some positive integer k, the characteristic polynomial of the Frobenius endomorphism π on A over $\mathbb{F}_q$ is given by $P(X) = (X \pm q^{k/2})^{2g}$.

(iii) For some positive integer k, $\#A(\mathbb{F}_q) = (q^{k/2} \pm 1)^{2g}$.

(iv) For some positive integer k, $\pi^k = \pm q^{k/2}$.

In terms of the Frobenius (condition (iv)), this theorem shows the notion of supersingularity for general varieties is the same as the notion of supersingularity fo elliptic curves. From a more practical standpoint, however, it is sometimes more useful to have an analogue of condition (iii) of Theorem 19, rather than condition (iv). To state such an analogue, we first list the following useful properties of the characteristic polynomial of Forbenius (see [21]).

Theorem 21. *Let C be a curve of genus g over a finite field $\mathbb{F}_q$, and let $P(X) = \prod_{i=1}^{2g}(X - \alpha_i)$ be the characteristic polynomial of the Frobenius endomorphism on the Jacobian of C. Then $P(X)$ satisfies the following conditions.*

(i) (Riemann Hypothesis): The roots of $P(X)$ are algebraic integers and all have modulus equal to $\sqrt{q}$.

(ii) The α_i come in complex conjugate pairs, so without loss of generality we may assume $\alpha_i\alpha_{i+g} = q$ for $1 \leq i \leq g$.

(iii) $P(X)$ can be written in the form

$$P(X) = X^{2g} + a_1X^{2g-1} + a_2X^{2g-2} + \ldots + a_gX^g + a_{g-1}qX^{g-1} + ... + a_1q^{g-1}X + q^g,$$

where the coefficients $a_i \in \mathbb{Z}$ are, up to sign, the elementary symmetric polynomials of the α_i.

(iv) For any $r \geq 1$,

$$\#C\left(\mathbb{F}_{q^r}\right) = q^r + 1 - t_r,$$

where $t_r = \sum_{i=1}^{2g} \alpha_i^r$.

(v) For any $r \geq 1$,

$$\#J\left(\mathbb{F}_{q^r}\right) = \prod_{i=1}^{2g}\left(1 - \alpha_i^r\right).$$

Bearing in mind statement (iii) of the previous theorem, we now state the analogue of Theorem 19 (proven in [21]):

Theorem 22. *Suppose A is an abelian variety of genus g over $\mathbb{F}_q$, $q = p^n$. Denote the characteristic polynomial of the Frobenius by*

$$P(X) = X^{2g} + a_1X^{2g-1} + a_2X^{2g-2} + \ldots + a_gX^g + a_{g-1}qX^{g-1} + ... + a_1q^{g-1}X + q^g.$$

Then A is supersingular if and only if

$$p^{\lceil rn/2 \rceil} \mid a_r$$

for $1 \leq r \leq g$.

It is possible to apply these fundamental results on supersingularity and higher genus curves to prove Theorem 4 in the arithmetic cases. In fact, one may make use of Theorem 21 to translate the problem of divisibility of the coefficients of $P(X)$ mod p given in Theorem 20 into a point counting problem for genus 2 curves over finite fields. This approach also requires some classical results on the mod p reduction of binomial coefficients (see [51, 62]). We avoid this approach, however, in favor of an argument treating all values of m simultaneously.

4.1.2. Hasse-Witt matrices and ordinary curves. The general case of $m \geq 3$ requires a bit more background. We first introduce some additional material from the study of hyperelliptic curves. For related references, see [18, 22, 55, 56, 76, 80].

Fix an algebraically closed field k of characteristic $p > 2$, and consider a hyperelliptic curve C defined over k given by a non-singular affine equation of the form

$$y^2 = f(x), \tag{4.1.1}$$

where $f(x)$ has degree $2g + 1$ or $2g + 2$, and g is the genus of the curve. One can easily compute the Hasse-Witt matrix A of C given the function f, by the following procedure. If we define the coefficients c_k by the equation

$$f(x)^{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}\deg f} c_k x^k, \tag{4.1.2}$$

then the Hasse-Witt matrix for A is the $g \times g$ matrix

$$A = [c_{ig-j}]_{i,j=1}^{g}.$$

Example 23. Consider an elliptic curve E over k of characteristic $p > 2$ given by an equation in Legendre normal form:

$$y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \neq 0, 1$. In this case, it is well known that the Hasse-Witt matrix reduces to the so-called Hasse invariant for E, given by the following polynomial in λ:

$$W(\lambda) = \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k}^2 \lambda^k.$$

See [5, 29, 68] for more information on this polynomial.

In the case of elliptic curves, the Hasse-Witt matrix detects supersingularity. More specifically, an elliptic curve given in Legendre normal form is supersingular if and only if λ is a root of the above polynomial. As we will see shortly, in the general case we are no longer detecting supersingularity, but there is a natural analogue of what happens in the elliptic curve case. First, we recall the following theorem proven in [80].

Theorem 24. *Let C be a hyperelliptic curve of genus g defined by an equation of the form (4.1.1) over the field $\mathbb{F}_{p^a}$ for some $a > 1$. Let $Jac(C)$ denote the Jacobian of C over this finite field, let π denote the Frobenius endomorphism of $J(C)$ relative to this finite field, let P_π denote the characteristic polynomial of*

π, let A denote the Hasse-Witt matrix of the curve, and let

$$A_\pi = AA^{(p)} \dots A^{\left(p^{a-1}\right)},$$

where

$$A^{(p^r)} = \left[c_{ig-j}^{p^r}\right]_{i,j=1}^{g},$$

i.e. the coefficients of $A^{(p^r)}$ are the p^r-th powers of the coefficients of A. Then the following statements are equivalent:

(i) $\det A_\pi \neq 0$.

(ii) $\det A \neq 0$, *i.e. A has rank g.*

(iii) $AA^{(p)} \dots A^{\left(p^{g-1}\right)}$ has rank g.

(iv) There are p^g points on Jac(C) killed by p in the algebraic closure of $\mathbb{F}_{p^a}$ (in other words, the p-rank of Jac(C) equals g).

(v) $P_\pi(\lambda)$ has g p-adic unit roots in $\overline{\mathbb{Q}}_p$.

There are other equivalent conditions listed in [80], but we shall not need them here. The theorem above motivates the following definition:

Definition 25. If any of the equivalent statements in Theorem 24 hold, the Jacobian Jac(C) is said to be ordinary, and we call C an ordinary curve.

As seen in the statement of Theorem 4, it is this notion of ordinariness that is captured by the roots of generalized Atkin-polynomials. It is proven in [80] that, in the notation of the above theorem, $A = 0$ is a sufficient condition for a curve to be supersingular, though not necessary. Of course, the condition $A = 0$ is much stronger than the condition that the curve is ordinary.

After proving some necessary preliminary lemmas, we will prove Theorem 4. We will then investigate the finitely many arithmetic cases, and will conclude with some examples and corollaries of the main result.

4.2. Preliminary results

There are several intermediate results that will be required to prove Theorem 4. Some of them can be stated and proven before we turn to the main result. Here we collect these necessary preliminaries.

We begin with an elementary lemma on the discriminants of the polynomials appearing in the family of curves $\mathcal{F}_m$.

Lemma 26. *(i) When $m \equiv 0$ mod 4, the discriminant of the polynomial $x\left(x^m - 2ax^{m/2} + b\right)$ is equal to*

$$m^m b^{\frac{m}{2}+1}(b-a^2)^{\frac{m}{2}}.$$

(ii) When $m \equiv 2 \bmod 4$, the discriminant of the polynomial $x^m - 2ax^{m/2} + b$ is equal to

$$-m^m b^{\frac{m}{2}-1}(b-a^2)^{\frac{m}{2}}.$$

(iii) When m is odd, the discriminant of the polynomial $x\left(x^{2m} - 2ax^m + b\right)$ is equal to

$$-(2m)^{2m} b^{m+1}(b-a^2)^m.$$

Proof. This follows by direct computation from a well known result (see, for example, Proposition 12.1.4 of [34]) that the discriminant of a degree n monic polynomial f with roots α_i is equal to

$$(-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

□

As a consequence of this result, a given curve in $\mathcal{F}_m$ is automatically singular over a field of characteristic p only if $p \mid 2m$. This is why we exclude such primes in the statement of Theorem 4.

Our next two results concern the reduction of certain multinomial coefficients mod p.

Lemma 27. *For $0 \le r \le \lfloor u/2 \rfloor$,*

$$4^{-r}\binom{\frac{p-1}{2}}{r, u-2r, \frac{p-1}{2}-u+r} \equiv \binom{\frac{p-1}{2}}{u} \frac{\left(-\frac{u}{2}\right)_r \left(-\frac{u}{2}+\frac{1}{2}\right)_r}{r!\left(-u+\frac{1}{2}\right)_r} \text{ mod } p.$$

Proof. First, when r equals 0, both sides are equal to $\binom{\frac{p-1}{2}}{u}$. Next, if the congruence holds for a whole number $r < \lfloor u/2 \rfloor$, then

$$\begin{aligned}
& 4^{-r-1}\binom{\frac{p-1}{2}}{r+1, u-2r-2, \frac{p-1}{2}-u+r+1} \\
= \; & 4^{-r}\binom{\frac{p-1}{2}}{r, u-2r, \frac{p-1}{2}-u+r} \frac{(u-2r)(u-2r-1)}{4(r+1)\left(\frac{p+1}{2}+r-u\right)} \\
\equiv \; & \binom{\frac{p-1}{2}}{u} \frac{\left(-\frac{u}{2}\right)_r \left(-\frac{u}{2}+\frac{1}{2}\right)_r}{r!\left(-u+\frac{1}{2}\right)_r} \frac{\left(-\frac{u}{2}+r\right)\left(-\frac{u}{2}+r+\frac{1}{2}\right)}{(r+1)\left(-u+r+\frac{1}{2}\right)} \\
= \; & \binom{\frac{p-1}{2}}{u} \frac{\left(-\frac{u}{2}\right)_{r+1} \left(-\frac{u}{2}+\frac{1}{2}\right)_{r+1}}{(r+1)!\left(-u+\frac{1}{2}\right)_{r+1}}.
\end{aligned}$$

Therefore, the result holds by induction. □

Lemma 28. *For any $1 \le u \le \frac{p-1}{2}$, we have*

$$(-2)^u \binom{\frac{p-1}{2}}{u} \equiv \frac{\left(\frac{1}{2}-u\right)_{\lfloor u/2 \rfloor}(-1)^{\lfloor u/2 \rfloor}}{\left\lfloor \frac{u}{2} \right\rfloor!} \text{ mod } p.$$

Proof. We prove the result by induction on u. When $u = 0$ or $u = 1$ the result is clear, as both sides are congruent to 1 mod p. For the induction step, we first note that

$$(-2)^{u+1}\binom{\frac{p-1}{2}}{u+1} = (-2)^u\binom{\frac{p-1}{2}}{u}\frac{(-2)\left(\frac{p-1}{2}-u\right)}{u+1}, \tag{4.2.1}$$

and then split into two cases.

Case 1: u even. In this case, the induction hypothesis combines with (4.2.1) to give us

$$\begin{aligned}(-2)^{u+1}\binom{\frac{p-1}{2}}{u+1} &\equiv \frac{\left(\frac{1}{2}-u\right)_{u/2}(-1)^{u/2}}{\frac{u}{2}!}\frac{2u+1}{u+1}\\ &= \frac{\left(\frac{1}{2}-(u+1)\right)_{u/2}(-1)^{u/2}}{\frac{u}{2}!},\end{aligned}$$

since

$$\frac{\left(\frac{1}{2}-(u+1)\right)_{u/2}}{\left(\frac{1}{2}-u\right)_{u/2}} = \frac{\frac{1}{2}-u-1}{\frac{1}{2}-u+\frac{u}{2}-1} = \frac{2u+1}{u+1}.$$

Case 2: u odd. In this case, again combining the induction hypothesis with (4.2.1), we see that

$$(-2)^{u+1}\binom{\frac{p-1}{2}}{u+1} \equiv \frac{\left(\frac{1}{2}-u\right)_{\frac{u-1}{2}}(-1)^{\frac{u-1}{2}}}{\frac{u-1}{2}!}\frac{2u+1}{u+1}.$$

This time, we have

$$\frac{2u+1}{u+1} = \frac{\frac{1}{2}+u}{\frac{u+1}{2}} = -\frac{\left(\frac{1}{2}-(u+1)\right)_{\frac{u+1}{2}}}{\left(\frac{1}{2}-u\right)_{\frac{u-1}{2}}\frac{u+1}{2}},$$

so the above expression simplifies to

$$\frac{\left(\frac{1}{2}-(u+1)\right)_{\frac{u+1}{2}}(-1)^{\frac{u+1}{2}}}{\frac{u+1}{2}!}.$$

Combining these two cases, we see the result holds by induction. □

We also need the following results on hypergeometric functions.

Lemma 29. *${}_2F_1(a,b;c;x)$ satisfies the same second order differential equation as ${}_2F_1(a,b;a+b+1-c;1-x)$.*

Proof. Both satisfy the hypergeometric differential equation (2.1.12) (the first is obvious, the second is a straightforward computation). □

Lemma 30. *The space of solutions to the hypergeometric differential equation (2.1.12) mod p has dimension 1 when $c = 1$, and is generated by ${}_2F_1(a,b;1;z)$.*

Proof. See p. 104 of [33]. □

Finally, we state a result on the congruence of certain generalized Atkin polynomials mod p.

Lemma 31. *Fix a prime p not dividing $2m$, and fix an i between 1 and $\lceil g/2 \rceil$. Let u, j, ϵ and k be as in the statement of Theorem 4, and let δ denote the residue of u modulo 2 (in other words, $\delta = u - 2\lfloor u/2 \rfloor$). Also, let $n_p = \left\lfloor \frac{u}{2} \right\rfloor + \delta + \epsilon$. Then*

$$\mathcal{A}_{n_p,m,k}(J) \equiv U^{\delta}_{n_p,m,k}(J) \equiv V^{\epsilon}_{n_p,m,k}(J) \ mod\ p.$$

Proof. We prove the result in the case that $m \equiv 0 \bmod 4$; the proof in the other cases is nearly identical. There are four cases to consider, though each case requires only a slight modification to the general argument.

Case 1: $\epsilon = \delta = 0$. In this case, $1 \leq j \leq m/4$ and u is even. Therefore, $n_p = \frac{(2i-1)p-2j+1}{2m}$, and $k = m/2 - 2j + 1$ so that $\alpha_{m,k} = \frac{2j-1}{2m}$ and therefore $p \mid (n_p + \alpha_{m,k})$. Hence, the coefficients of all but the first term in the first and third sums in Proposition 15 are divisible by p, and

$$\mathcal{A}_{n_p,m,k}(J) \equiv U^{0}_{n_p,m,k}(J) \equiv V^{0}_{n_p,m,k}(J) \bmod p.$$

Case 2: $\epsilon = 0$, $\delta = 1$. In this case, $1 \leq j \leq m/4$ and u is odd. Now $n_p = \frac{(2i-1)p-2j+1}{2m} + \frac{1}{2}$ and once again $\alpha_{m,k} = \frac{2j-1}{2m}$, so that in this case $p \mid (n_p - \beta_{m,k})$. This time, the coefficients of all but the first term in the second and third sums in Proposition 15 are divisible by p, and the result follows as in the first case.

Case 3: $\epsilon = 1$, $\delta = 0$. Now $m/4 + 1 \leq j \leq m/2$ and u is even, so that $n_p = \frac{(2i-1)p-2j+1}{2m} + 1$ but now $\beta_{m,k} = \frac{2j-1}{2m}$. In this case, $p \mid (n_p + \beta_{m,k} - 1)$. This time, the coefficients of all but the first term in the first and fourth sums in Proposition 15 are divisible by p, and the result follows as before.

Case 4: $\epsilon = 1$, $\delta = 1$. In this case $m/4 + 1 \leq j \leq m/2$ and u is odd, so $n_p = \frac{(2i-1)p-2j+1}{2m} + \frac{3}{2}$ and $\beta_{m,k} = \frac{2j-1}{2m}$. In this case, $p \mid (n_p - \alpha_{m,k} - 1)$. This time, the coefficients of all but the first term in the second and fourth sums in Proposition 15 are divisible by p, and the proof is complete. □

4.3. Proof of Theorem 4

We prove the result in full generality, though the notation can be somewhat cumbersome. The interested reader can easily specify to one of the cases m odd, $m \equiv 0 \bmod 4$, or $m \equiv 2 \bmod 4$ for a slightly clearer (though less general) explanation.

To prove Theorem 4, it suffices to show that the roots of the generalized Atkin polynomials $\mathcal{A}_{n_p,m,k}(J)$ mod p correspond to curves whose Hasse-Witt matrix A fails to have full rank. The bridge between zeros of the polynomials and entries of A is formed via hypergeometric functions.

To begin, consider the Hasse-Witt matrix of a curve C given by the equation

$$C:\ y^2 = x^{2g+1+\kappa_m} - 2ax^{g+1} + bx^{1-\kappa_m} \tag{4.3.1}$$

over some finite field F of characteristic $p > 2$. Since we assume p does not divide $2m$, we know by Lemma 26 that this curve is nonsingular over F provided $b \neq 0$ and $b - a^2 \neq 0$. We have assumed the latter condition always holds in our definition of $\mathcal{F}_m$, but we will need to study the singular case $b = 0$ at the end of the argument. For the moment, though, assume $b \neq 0$ too, so that this is indeed a non-singular curve. Since this curve is hyperelliptic, and since we know the degree of the polynomial on the right hand side equals $2g + 1 + \kappa_m$, the genus of such a curve is g, and therefore the Hasse-Witt matrix A will be a $g \times g$ matrix. This follows from the well-known genus formula for hyperelliptic curves, namely that if

$$y^2 = f(x)$$

represents a hyperelliptic curve with $\deg f = 2g + 1$ or $2g + 2$, then g is the genus. Our first goal is to give a proof of the following proposition:

Proposition 32. *Fix the notation as in the statement of Theorem 4. When $b \neq 0$, the entries c_{ip-j} of the Hasse-Witt matrix A associated to C are zero unless j satisfies (1.0.2). In particular, there can be at most one non-zero entry in each row of the Hasse-Witt matrix, and for each $1 \leq i \leq \lceil g/2 \rceil$, the only possible nonzero entry in the ith row satisfies the following equality over F:*

$$c_{ip-j} = \left(\frac{-2a}{b}\right)^u b^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{u} {}_2F_1\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4(g+\kappa_m)} + \frac{1}{2}; \frac{2j+\kappa_m-1}{2(g+\kappa_m)} + \frac{1}{2}; \frac{J}{J-1}\right),$$

where u is given by (1.0.1).

To prove this result, we first observe that the degrees of the terms on the right hand side of (4.3.1) differ by at least g. This means each row of A can have at most one nonzero entry. More specifically, if we set $f(x) = x^{2g+1+\kappa_m} - 2ax^{g+1} + bx^{1-\kappa_m}$, then

$$f(x)^{\frac{p-1}{2}} = \sum_{\substack{r,s,t\geq 0 \\ r+s+t=\frac{p-1}{2}}} \binom{\frac{p-1}{2}}{r,s,t} (-2a)^s b^t x^{r(2g+1+\kappa_m)+s(g+1)+t(1-\kappa_m)}.$$

Recalling the notation from (4.1.2), we have

$$c_{ip-j} = \sum_{\substack{r+s+t=\frac{p-1}{2} \\ r(2g+1+\kappa_m)+s(g+1)+t(1-\kappa_m)=ip-j \\ r,s,t\geq 0}} \binom{\frac{p-1}{2}}{r,s,t} (-2a)^s b^t.$$

If we fix r, the conditions on r, s, and t imply

$$\begin{aligned} r &= r, \\ s &= \frac{(2i+\kappa_m-1)\,p-2j+1-\kappa_m}{2\,(g+\kappa_m)}-2r, \\ t &= \frac{p-1}{2}+r-\frac{(2i+\kappa_m-1)\,p-2j+1-\kappa_m}{2\,(g+\kappa_m)}. \end{aligned}$$

In particular, since r, s, and t must be nonnegative integers, $c_{ip-j}=0$ unless

$$\frac{(2i+\kappa_m-1)\,p-2j+1-\kappa_m}{2\,(g+\kappa_m)} \tag{4.3.2}$$

is an integer. But this is precisely the statement that j is given by (1.0.2), since $1\le j\le g$. Therefore, for each i, j is uniquely determined by the expression given in the statement of Theorem 4, and we see that each row of A can have at most one nonzero entry. This proves the first part of the proposition. Note that for this choice of j, (4.3.2) is just the number u defined by (1.0.1). We also note for future reference that $1\le i,j\le g$ implies $u\le p-1$.

We can further simplify the expression for c_{ip-j} by using the fact that each of the integers r, s, and t must lie between 0 and $\frac{p-1}{2}$. In terms of r and u, we then get three inequalities:

$$\begin{aligned} 0\le\ & r \le \frac{p-1}{2} \\ \frac{u}{2}-\frac{p-1}{4}\le\ & r \le \frac{u}{2} \\ u-\frac{p-1}{2}\le\ & r \le u. \end{aligned}$$

This implies that

$$\begin{aligned} c_{ip-j} &= \sum_{r=\max\left\{0,u-\frac{p-1}{2}\right\}}^{\lfloor u/2\rfloor} \binom{\frac{p-1}{2}}{r,\,u-2r,\,\frac{p-1}{2}-u+r} (-2a)^s\, b^t \\ &= \left(\frac{-2a}{b}\right)^u b^{\frac{p-1}{2}} \sum_{r=\max\left\{0,u-\frac{p-1}{2}\right\}}^{\lfloor u/2\rfloor} 4^{-r} \binom{\frac{p-1}{2}}{r,\,u-2r,\,\frac{p-1}{2}-u+r} \left(\frac{J}{J-1}\right)^r. \end{aligned} \tag{4.3.3}$$

We continue to analyze the c_{ip-j} with the following lemma.

Lemma 33. *Let $i'=g+1-i$, $j'=g+1-j$. Then for $1\le i\le\lceil g/2\rceil$,*

$$b^{\frac{p-1}{2}-u}c_{i'p-j'}=c_{ip-j}.$$

Proof. First, note that if we let u' denote the transformation of u when i goes to $i'$and j goes to j', then a straightforward calculation shows $u + u' = p - 1$. Also, note that if $i \leq \lceil g/2 \rceil$, $u \leq \frac{p-1}{2}$. Therefore,

$$\begin{aligned} b^{\frac{p-1}{2}-u} c_{i'p-j'} &= \left(\frac{-2a}{b}\right)^{u'} b^{p-1-u} \sum_{r=u'-\frac{p-1}{2}}^{\lfloor u'/2 \rfloor} 4^{-r} \binom{\frac{p-1}{2}}{r, u'-2r, \frac{p-1}{2}-u'+r} \left(\frac{J}{J-1}\right)^r \\ &= (-2a)^{p-1-u} \sum_{r=\frac{p-1}{2}-u}^{\lfloor \frac{p-1}{2}-\frac{u}{2} \rfloor} 4^{-r} \binom{\frac{p-1}{2}}{r, p-1-u-2r, u+r-\frac{p-1}{2}} \left(\frac{J}{J-1}\right)^r . \end{aligned}$$

Setting $R = r + u - \frac{p-1}{2}$, this expression becomes

$$\begin{aligned} & (-2a)^{p-1-u} \sum_{R=0}^{\lfloor \frac{u}{2} \rfloor} 4^{-R+u-\frac{p-1}{2}} \binom{\frac{p-1}{2}}{R-u+\frac{p-1}{2}, u-2R, R} \left(\frac{J}{J-1}\right)^{R-u+\frac{p-1}{2}} \\ = \;& (-2a)^{p-1-u}\, 4^{u-\frac{p-1}{2}} \left(\frac{J}{J-1}\right)^{\frac{p-1}{2}-u} b^{u-\frac{p-1}{2}} c_{ip-j} \\ = \;& c_{ip-j}, \end{aligned}$$

since $\frac{J}{J-1} = \frac{b}{a^2}$. □

In particular, this lemma shows the rank of A is determined by just $\lceil g/2 \rceil$ coefficients, not g as it might initially seem. This is why it suffices to give the formula for c_{ip-j} in Proposition 32 only for the case $1 \leq i \leq \lceil g/2 \rceil$. Notice also that g is even if and only if m is even.

Our proof of the main proposition is now nearly complete. By combining (4.3.3) with Lemma 27, we find that for $1 \leq i \leq \lceil g/2 \rceil$, since $u \equiv \frac{1-2j-\kappa_m}{2(g+\kappa_m)}$ mod p, the following chain of equality holds in the field F:

$$\begin{aligned} c_{ip-j} &= \left(\frac{-2a}{b}\right)^u b^{\frac{p-1}{2}} \sum_{r=0}^{\lfloor u/2 \rfloor} 4^{-r} \binom{\frac{p-1}{2}}{r, u-2r, \frac{p-1}{2}-u+r} \left(\frac{J}{J-1}\right)^r \\ &= \left(\frac{-2a}{b}\right)^u b^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{u} \sum_{r=0}^{\lfloor u/2 \rfloor} \frac{\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}\right)_{r+1} \left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}+\frac{1}{2}\right)_{r+1}}{(r+1)!\left(\frac{2j+\kappa_m-1}{2(g+\kappa_m)}+\frac{1}{2}\right)_{r+1}} \left(\frac{J}{J-1}\right)^r \\ &= \left(\frac{-2a}{b}\right)^u b^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{u} {}_2F_1\left(\frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}+\frac{1}{2}; \frac{2j+\kappa_m-1}{2\,(g+\kappa_m)}+\frac{1}{2}; \frac{J}{J-1}\right), \end{aligned}$$

by definition of the hypergeometric series, and the fact that either

$$\left(\frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}\right)_{\lfloor u/2 \rfloor + 1}$$

or

$$\left(\frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}+\frac{1}{2}\right)_{\lfloor u/2 \rfloor + 1}$$

equals zero in F. This completes the proof of the proposition.

We now have a bridge between the Hasse-Witt matrix A and hypergeometric functions. To complete the proof of Theorem 4, we therefore need to connect this bridge to generalized Atkin polynomials. To help make this connection, we use the remaining lemmas from the previous section.

Because the hypergeometric function appearing in Proposition 32 is a polynomial of degree $\lfloor u/2 \rfloor$ in $\frac{J}{J-1}$ over a field of characteristic p, we can write the above as

$$c_{ip-j} = \left(\frac{a}{b}\right)^u b^{\frac{p-1}{2}} (J-1)^{-\lfloor u/2 \rfloor} P_{p,m,j}(J),$$

where

$$P_{p,m,j}(J) = (-2)^u \binom{\frac{p-1}{2}}{u} (J-1)^{\lfloor u/2 \rfloor} {}_2F_1\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4(g+\kappa_m)} + \frac{1}{2}; \frac{2j+\kappa_m-1}{2(g+\kappa_m)} + \frac{1}{2}; \frac{J}{J-1}\right)$$

is a polynomial in J. Meanwhile, since $J-1 = \frac{a^2}{b-a^2}$, we can write the remaining part of c_{ip-j} as

$$b^{\frac{p-1}{2}-u} \left(b-a^2\right)^{\lfloor u/2 \rfloor} a^{\delta}.$$

Since b and $b-a^2$ are assumed to be nonzero, this is only zero if $a=0, \delta=1$ (note this is equivalent to $J=1, \delta=1$). Thus, we conclude that

$$c_{ip-j} = b^{\frac{p-1}{2}-u} \left(b-a^2\right)^{\lfloor u/2 \rfloor} a^{\delta} P_{p,m,j}(J).$$

We now split into two cases, depending on the size of j.

Case 1: $1 \le j \le \lceil g/2 \rceil$. In this case, by Lemma 31 we have

$$\mathcal{A}_{n_p,m,k}(J) = V^0_{n_p,m,k}(J)$$

over F, where $k = \frac{(2,m)}{2}(g+1-2j)$ so that $\frac{2j+\kappa_m-1}{4(g+\kappa_m)} = \alpha_{m,k}$. By definition of $V^0_{n_p,m,k}$

$$\begin{aligned} V^0_{n_p,m,k}(J) &= (J-1)^{n_p} {}_2F_1\left(\alpha_{m,k}, 1-\beta_{m,k}; 1; \frac{1}{1-J}\right) \\ &= (J-1)^{n_p} {}_2F_1\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4(g+\kappa_m)} + \frac{1}{2}; 1; \frac{1}{1-J}\right) \end{aligned}$$

over F. On the other hand, by Lemma 29,

$${}_2F_1\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4(g+\kappa_m)} + \frac{1}{2}; 1; x\right)$$

and

$${}_2F_1\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4(g+\kappa_m)} + \frac{1}{2}; \frac{2j+\kappa_m-1}{2(g+\kappa_m)} + \frac{1}{2}; 1-x\right)$$

satisfy the same second order hypergeometric differential equation. Since the third argument in the former function equals 1, Lemma 30 implies that the space of solutions over $\mathbb{F}_p$ to the corresponding hypergeometric differential equation has dimension 1, and therefore the two functions must agree up to a multiplicative constant. Evaluating at $J = 1$ and applying Lemma 28,

$$\begin{aligned} P_{p,m,j}(1) &= (-2)^u \binom{\frac{p-1}{2}}{u} \frac{\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}\right)_{\lfloor u/2\rfloor} \left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}+\frac{1}{2}\right)_{\lfloor u/2\rfloor}}{\left(\frac{2j+\kappa_m-1}{2(g+\kappa_m)}+\frac{1}{2}\right)_{\lfloor u/2\rfloor} \lfloor \frac{u}{2}\rfloor!} \\ &= \frac{\left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}\right)_{\lfloor u/2\rfloor} \left(\frac{2j+\kappa_m-1}{4(g+\kappa_m)}+\frac{1}{2}\right)_{\lfloor u/2\rfloor} (-1)^{\lfloor u/2\rfloor}}{\left(\lfloor \frac{u}{2}\rfloor!\right)^2} \\ &= \left.\frac{V^0_{n_p,m,k}(J)}{(J-1)^\delta}\right|_{J=1} \end{aligned}$$

over the field F. This determines the multiplicative constant, and more importantly shows that $P_{p,m,j}(J) = \frac{V^0_{n_p,m,k}(J)}{(J-1)^\delta}$. Therefore,

$$c_{ip-j} = b^{\frac{p-1}{2}-u}(b-a^2)^{\lfloor u/2\rfloor} a^\delta \frac{\mathcal{A}_{n_p,m,k}(J)}{(J-1)^\delta}.$$

In particular, $c_{ip-j} = 0$ in F precisely when $\mathcal{A}_{n_p,m,k}(J) = 0$ (notice that in the case $\delta = 1$, $(J-1) \mid \mathcal{A}_{n_p,m,k}(J)$, but $J = 1$ is still a root of $P_{p,m,j}$ since $J = 1$ if and only if $a = 0$).

Case 2: $\lceil g/2\rceil + 1 \leq j \leq g$. In this case, by Lemma 31 we have

$$\mathcal{A}_{n_p,m,k}(J) = V^1_{n_p,m,k}(J)$$

over F, where $-k = \frac{(2,m)}{2}(g+1-2j)$ so that $\frac{2j+\kappa_m-1}{4(g+\kappa_m)} = \beta_{m,k}$. By definition of $V^1_{n_p,m,k}$ we see that

$$\begin{aligned} V^{(1)}_{n_p,m,k}(J) &= J\,(J-1)^{n_p-1}\,{}_2F_1\left(\beta_{m,k}, 1-\alpha_{m,k}; 1; \frac{1}{1-J}\right) \\ &= J\,(J-1)^{n_p-1}\,{}_2F_1\left(\frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}, \frac{2j+\kappa_m-1}{4\,(g+\kappa_m)}+\frac{1}{2}; 1; \frac{1}{1-J}\right). \end{aligned}$$

Note the hypergeometric function is the same as in case 1. Also as in case 1, by Lemma 28 we have

$$P_{p,m,j}(1) = \left.\frac{V^1_{n_p,m,k}(J)}{J(J-1)^\delta}\right|_{J=1},$$

and so

$$c_{ip-j} = b^{\frac{p-1}{2}-u}(b-a^2)^{\lfloor u/2\rfloor} a^\delta \frac{\mathcal{A}_{n_p,m,k}(J)}{J(J-1)^\delta}.$$

Once again, $c_{ip-j} = 0$ in F precisely when $\mathcal{A}_{n_p,m,k}(J) = 0$, except possibly at the root $J = 0$.

We need to treat the root $J = 0$ separately, since this implies $b = 0$, and in our argument we have assumed throughout that $b \neq 0$. But in the case $b = 0$, $a \neq 0$ since $b - a^2 \neq 0$, so the equation of the curve reduces to

$$y^2 = x^{g+1}\left(x^{g+\kappa_m} - 2a\right).$$

By making use of the birational transformation $y \to yx^{\lfloor (g+1)/2 \rfloor}$, we see that C is birationally equivalent to a curve of the form

$$y^2 = x^{g+1-2\lfloor (g+1)/2 \rfloor}\left(x^{g+\kappa_m} - 2a\right).$$

Note the exponent on x is 0 if m is odd, and is 1 otherwise; in other words, the exponent can be written more succinctly as $(2, m) - 1$.

This is still hyperelliptic, so the genus of the curve decreases from the value g to $\lfloor g/2 \rfloor$. Therefore, the entries c_{ip-j} of the Hasse-Witt matrix satisfy $1 \leq i, j \leq \lfloor g/2 \rfloor$. Moreover, writing $f(x) = x^{(2,m)-1}\left(x^{g+\kappa_m} - 2a\right)$, we obtain

$$f(x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}((2,m)-1)} \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} x^{r(g+\kappa_m)} (-2a)^{\frac{p-1}{2}-r},$$

and so to find c_{ip-j} we must solve $ip - j = \frac{p-1}{2}\left((2,m)-1\right) + r\left(g+\kappa_m\right)$.

Fix i between 1 and $\lfloor g/2 \rfloor$. Then

$$r = \frac{ip - j - \frac{p-1}{2}\left((2,m)-1\right)}{g+\kappa_m},$$

and because r must be an integer, this forces

$$j \equiv ip - \frac{p-1}{2}\left((2,m)-1\right) \bmod g+\kappa_m.$$

Therefore, if the solution to this equivalence lies between 1 and $\lfloor g/2 \rfloor$, then there exists a j corresponding to i such that

$$c_{ip-j} = \binom{\frac{p-1}{2}}{r} (-2a)^{\frac{p-1}{2}-r} \neq 0.$$

However, it may be that the solution to the above equivalence is not in the range between 1 and $\lfloor g/2 \rfloor$. In this case, i.e. for $j \geq \lfloor g/2 \rfloor + 1$, the value of r is never integral, meaning that $c_{ip-j} = 0$.

In other words, when $b = 0$, the curve (of genus $\lfloor g/2 \rfloor$) is non-ordinary precisely when there exists some i between 1 and $\lfloor g/2 \rfloor$ for which the corresponding value of j is larger than $\lfloor g/2 \rfloor$. When m is even, this puts us in the second case above, so that whenever j is larger than $\lfloor g/2 \rfloor$ we have both $c_{ip-j} = 0$ and

$$\mathcal{A}_{n_p,m,k}(J) = V^1_{n_p,m,k}(J)$$

over F, from which it follows that when $b = 0$, $J = 0$, and therefore $\mathcal{A}_{n_p,m,k}(J) = 0$, since J is a root of $V^1_{n_p,m,k}$. When m is odd, we are once again in the second case above unless $j = \frac{g+1}{2}$, which cannot happen.

So in either case, for fixed i between 1 and $\lfloor g/2 \rfloor$, if the corresponding j value is larger than $\lfloor g/2 \rfloor$, the root of c_{ip-j} is matched by a root of $\mathcal{A}_{n_p,m,k}(J)$. In other words, regardless of the value of b, the roots of c_{ip-j} coincide with the roots of $\mathcal{A}_{n_p,m,k}(J)$.

We claim the proof is now complete. To see why, note that whenever $c_{ip-j} = 0$, this means the curve is non-ordinary. Since the zeros of each c_{ip-j} correspond to the zeros of $\mathcal{A}_{n_p,m,k}(J)$, this implies that the Atkin-type polynomials are detecting whether or not the curve is ordinary. In fact, the argument of this proof allows us to say a bit more; indeed, if J is a root of $\mathcal{P}_{m,p}$, we see that the rank of the Hasse-Witt matrix typically decreases by two times the multiplicity of the root (though some extra care must be taken in the case of m odd). We will summarize this statement in a corollary in the next section.

4.4. Corollaries and examples

In this section, we give corollaries and numerical examples based on the ideas of this chapter. The results are grouped into two collections, depending on whether or not G_m is arithmetic.

4.4.1. The arithmetic cases. Though for general m we have shown the polynomials $\mathcal{A}_{n,m,k}$ do not detect supersingularity, we claim that in the cases when G_m is arithmetic, supersingularity is still detected. When $m = 3$ this is the original result due to Atkin, and when $m = \infty$ the curves are again elliptic (see below for more on this case). In the cases $m = 4$ and $m = 6$ one can prove this using the information on supersingular curves provided in Section 4.1.1, though it is easier to use the following result regarding hyperelliptic curves of genus 2 (see [31, 52, 55, 80] for more details).

Proposition 34. *Consider the curve C over an algebraically closed field of characteristic $p > 2$ given by the non-singular affine equation*

$$y^2 = f(x),$$

where $\deg f = 5$ *or* 6 *(so that the genus equals 2). Let c_j denote the coefficient of x^j in $f(x)^{\frac{p-1}{2}}$. Then C is supersingular if and only if*

$$M^{(p)}M = 0,$$

where

$$\begin{aligned} M &= \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix} \\ M^{(p)} &= \begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix}. \end{aligned}$$

Note M is the Hasse-Witt matrix of the curve. Combining the proof of Theorem 4 with this proposition, it follows that C is supersingular if and only if either $c_{p-1} = 0$ or $c_{p-2} = 0$. In either case, this vanishing is controlled by the zeros of certain generalized Atkin polynomials. A more precise statement is provided by Corollary 5.

A second corollary gives us simple formulas for the number of supersingular curves appearing in each of the arithmetic cases $m = 4, 6, \infty$ (the case $m = 3$ is discussed in [40]).

Corollary 35. *Over an algebraically closed field of characteristic $p > 3$,*

(i) The number of supersingular curves (up to isogeny) given by an equation of the form $y^2 = x^5 - 2ax^3 + bx$ with $b - a^2 \neq 0$ is finite; more specifically, the number of curves equals $\left\lceil \frac{p-1}{4} \right\rceil - \left\lfloor \frac{p-1}{8} \right\rfloor$.

(ii) The number of supersingular curves (up to isogeny) given by an equation of the form $y^2 = x^6 - 2ax^3 + b$ with $b - a^2 \neq 0$ is finite; more specifically, the number of curves equals $\left\lceil \frac{p-1}{3} \right\rceil - \left\lfloor \frac{p-1}{6} \right\rfloor$.

(ii) The number of supersingular elliptic curves (up to isogeny) given in Jacobi quartic form by $y^2 = x^4 - 2ax^2 + 1$ with $a^2 \neq 1$ equals $\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$.

We now present the following examples in the arithmetic cases.

Example 36. Here is a simple numerical example. Consider the case $m = 4, p = 17$. In this case, $n_p = 2$, and by Theorem 3 we see

$$\begin{aligned} \mathcal{A}_{2,4}(J) &= J^2 - \frac{89}{96}J + \frac{77}{1024} \\ &\equiv (J-13)(J-9) \bmod 17. \end{aligned}$$

On the other hand, we know that a curve defined by the equation $y^2 = x^5 - 2ax^3 + bx$ with $b - a^2 \neq 0$ is supersingular precisely when the coefficient c_{16} of x^{16} in $\left(x^5 - 2ax^3 + bx\right)^8$ vanishes. By direct computation, we see

$$\begin{aligned} c_{16} &= 1120a^4b^4 + 672a^2b^5 + 28b^6 \\ &\equiv b^4\left(b - a^2\right)^2 (J-13)(J-9) \bmod 17. \end{aligned}$$

In other words, the J invariants corresponding to supersingularity are precisely the roots of the Atkin-type polynomial $\mathcal{A}_{2,4}$.

Example 37. Occasionally the same generalized Atkin polynomial must serve as the reduction of the supersingular polynomial $ss_{p,4}$ for as many as four different primes. For example, n_p equals 14 for each of the four primes 103, 107, 109, and 113 (congruent modulo 8 to 7, 3, 5, and 1, respectively). The Atkin-type polynomial $\mathcal{A}_{14,4}(J)$ is given by

$$\begin{aligned}\mathcal{A}_{14,4}(J) = J^{14} &- \frac{6005}{864}J^{13} + \frac{10325333}{479232}J^{12} - \frac{1004047363}{25559040}J^{11} + \frac{58756352298721}{1256277934080}J^{10} \\ &- \frac{11763949555530799}{308206853160960}J^{9} + \frac{28675267746952015}{1315015906820096}J^{8} - \frac{5522397073788267503}{631207635273646080}J^{7} \\ &+ \frac{1679637535061612479575}{689447059754894491648}J^{6} - \frac{439175894232756927495}{959230691832896684032}J^{5} + \frac{61077088654582048833667}{1105033756991496980004864}J^{4} \\ &- \frac{357405887139940300280 5}{9066943647109718810296 32}J^{3} + \frac{282979016976598806965816 3}{1980704062856608439838598758 4}J^{2} \\ &- \frac{3624642993287496622187963}{1901475900342344102245054808064}J + \frac{5391153289064591138944 7}{2028240960365167042394725128601 6}.\end{aligned}$$

By Theorem 5, the reduction of this polynomial modulo the four primes listed above gives the mod p reduction of the supersingular polynomials $ss_{103,4}(J)$, $ss_{107,4}(J)$, $ss_{109,4}(J)$, and $ss_{113,4}(J)$. These are

$$\begin{aligned} ss_{103,4}(J) &\equiv J(J+15)(J+20)(J+32)(J+48)(J+53)(J+54) \\ &\quad \times(J+67)(J+71)(J+102)(J^2+33J+25)(J^2+63J+64) \bmod 103, \\ ss_{107,4}(J) &\equiv J(J+3)(J+26)(J+34)(J+48)(J+61)(J^2+13J+62) \\ &\quad \times(J^2+37J+49)(J^2+86J+23)(J^2+105J+34) \bmod 107, \\ ss_{109,4}(J) &\equiv (J+28)(J+100)(J+106)(J+108)(J^2+3J+25)(J^2+13J+66) \\ &\quad \times(J^2+47J+49)(J^2+54J+89)(J^2+60J+5) \bmod 109, \\ ss_{113,4}(J) &\equiv (J+4)(J+32)(J+50)(J+104)(J^2+21J+8)(J^2+66J+106) \\ &\quad \times(J^2+91J+53)(J^2+108J+56)(J^2+112J+7) \bmod 113. \end{aligned}$$

On the other hand, for $m = 6, \infty$, the same generalized Atkin polynomial need only serve as the mod p reduction for as many as two different supersingular polynomials. To see an example in each case, note that when $m = 6$, $n_p = 3$ for both $p = 11$ and $p = 19$. We have

$$\mathcal{A}_{3,6}(J) = J^3 - \frac{64}{45}J^2 + \frac{511}{1080}J - \frac{77}{5832}.$$

Reducing this polynomial modulo the two primes given above, we find

$$\begin{aligned} ss_{11,6}(J) &\equiv J(J-1)(J+3) \bmod 11, \\ ss_{19,6}(J) &\equiv (J+17)(J^2+J+9) \bmod 19. \end{aligned}$$

Similarly, when $m = \infty$, $n_p = 3$ for both $p = 11$ and $p = 13$. The generalized Atkin polynomial takes the form

$$\mathcal{A}_{3,\infty}(J) = J^3 - \frac{7}{5}J^2 + \frac{4579}{10240}J - \frac{63}{8192}.$$

Reducing this polynomial modulo these primes yields

$$\begin{aligned} ss_{11,\infty}(J) &\equiv (J-1)(J+7)(J+8) \bmod 11, \\ s_{13,\infty}(J) &\equiv (J+1)(J^2+8J+1) \bmod 13. \end{aligned}$$

Example 38. Since the curves in the $m = 3$ and the $m = \infty$ case are elliptic curves, it is possible define the supersingular polynomial $ss_{p,\infty}$ in terms of $ss_{p,3}$ by using the well-known relation between J_3 and J_∞ given by (see [60])

$$J_3 = \frac{(4J_\infty - 1)^3}{27J_\infty}. \tag{4.4.1}$$

Following the type of argument found in [75] for the development of Atkin-type polynomials for congruence subgroups of G_3 with low level, for a fixed prime greater than 3 we set

$$ss^{new}_{p,\infty}(J_\infty) = \prod_{\substack{E/\overline{\mathbb{F}}_p \\ J_3(E) \text{ determined by} \\ J_\infty(E) \text{ is supersingular}}} (J_\infty - J_\infty(E)).$$

Here we are viewing J_∞ as a variable, and $J_\infty(E)$ as the J_∞ invariant of a fixed elliptic curve (and similarly for J_3 compared to $J_3(E)$).

Using (4.4.1), notice that

$$\begin{aligned} ss_{p,3}(J_3) &= \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (J_3 - J_3(E)) \\ &= \prod \left(\frac{(4J_\infty - 1)^3}{27J_\infty} - \frac{(4J_\infty(E) - 1)^3}{27J_\infty(E)} \right), \end{aligned}$$

so that if we set $n_p = \deg ss_p(J_3)$,

$$\begin{aligned} &\left(\frac{27}{64}J_\infty\right)^{n_p} ss_{p,3}\left(\frac{(4J_\infty - 1)^3}{27J_\infty}\right) \\ &= \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} \left((J_\infty - 1/4)^3 - (J_\infty(E) - 1/4)^3 \frac{J_\infty}{J_\infty(E)} \right). \end{aligned} \tag{4.4.2}$$

Also, notice that if we view

$$(4J_\infty - 1)^3 - 27J_3J_\infty = 0$$

as a polynomial in J_∞, the discriminant of this polynomial equals $2^8 3^9 J_3^2 (J_3 - 1)$, so that for a fixed J_3, the solutions J_∞ of (4.4.1) are distinct provided $J_3 \neq 0, 1$. When $J_3 = 0$, we get one root with multiplicity 3, and when $J_3 = 1$, the solutions J_∞ satisfy $(J_\infty - 1)(8J_\infty + 1)^2$, so that we get one simple root and one double root.

To understand the relevancy of the above observations, notice that by the definition of $ss_{p,\infty}^{new}$, it divides the polynomial given by (4.4.2). On the other hand, we know that the degree of $ss_{p,\infty}^{new}$ equals $\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$, in other words the degree equals $\frac{p\pm1}{4}$, depending on the residue of p mod 4. Therefore, if $p \equiv 1 \bmod 12$, $n_p = \frac{p-1}{12}$ so that (4.4.2) and $ss_{p,\infty}^{new}$ have the same degree and are monic. We therefore conclude

$$ss_{p,\infty}^{new}(J_\infty) = \left(\frac{27}{64} J_\infty\right)^{n_p} ss_{p,3}\left(\frac{(4J_\infty - 1)^3}{27 J_\infty}\right).$$

If $p \equiv 5 \bmod 12$, we need to divide out by the multiple roots to ensure that (4.4.2) is square free. With this added consideration, we find that

$$ss_{p,\infty}^{new}(J_\infty) = \frac{1}{(J_\infty - 1/4)^2} \left(\frac{27}{64} J_\infty\right)^{n_p} ss_{p,3}\left(\frac{(4J_\infty - 1)^3}{27 J_\infty}\right).$$

Similarly, if $p \equiv 7 \bmod 12$, we have

$$ss_{p,\infty}^{new}(J_\infty) = \frac{1}{(J_\infty + 1/8)} \left(\frac{27}{64} J_\infty\right)^{n_p} ss_{p,3}\left(\frac{(4J_\infty - 1)^3}{27 J_\infty}\right),$$

and for $p \equiv 11 \bmod 12$, we have

$$ss_{p,\infty}^{new}(J_\infty) = \frac{1}{(J_\infty - 1/4)^2 (J_\infty + 1/8)} \left(\frac{27}{64} J_\infty\right)^{n_p} ss_{p,3}\left(\frac{(4J_\infty - 1)^3}{27 J_\infty}\right).$$

We can use these identities to prove that this new supersingular polynomial agrees with the one originally introduced, though to do this requires the cubic transformation formulae proven in [75]:

$${}_2F_1\left(\frac{1}{4}, \frac{3}{4}; 1; x\right) = \begin{cases} {}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; \frac{27x(1-x)^2}{(1+3x)^3}\right)(1+3x)^{\frac{p-1}{4}}, & p \equiv 1 \bmod 4, \\ {}_2F_1\left(\frac{7}{12}, \frac{11}{12}; 1; \frac{27x(1-x)^2}{(1+3x)^3}\right)(1+3x)^{\frac{p-7}{4}}(9x-1), & p \equiv 3 \bmod 4. \end{cases}$$

Consider the case $p \equiv 1 \bmod 12$. By the lemmas in Section 4.2 and the known result on zeros of Atkin polynomials, over $\mathbb{F}_p$ we have

$$\begin{aligned} ss_{p,\infty}^{new}\left(J_\infty\right) &= \left(\frac{27}{64}J_\infty\right)^{n_p} U^0_{n_p,3}\left(\frac{\left(4J_\infty - 1\right)^3}{27J_\infty}\right) \\ &= \left(J_\infty - 1/4\right)^{3n_p} {}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; \frac{27J_\infty}{\left(4J_\infty - 1\right)^3}\right) \\ &= \left(\frac{J-1}{4}\right)^{3n_p} {}_2F_1\left(\frac{1}{4}, \frac{3}{4}; 1; \frac{J_\infty}{J_\infty - 1}\right) \\ &= (J-1)^{3n_p} {}_2F_1\left(\frac{1}{4}, \frac{3}{4}; 1; \frac{1}{1-J_\infty}\right) \\ &= V^0_{\frac{p-1}{4},\infty}\left(J_\infty\right) = \mathcal{A}_{\frac{p-1}{4},\infty}\left(J_\infty\right) = ss_{p,\infty}\left(J_\infty\right). \end{aligned}$$

Similar arguments can be made in the remaining cases. We summarize this relationship between $ss_{p,3}$ and $ss_{p,\infty}$ in the following corollary.

COROLLARY 39. *The relationship between $ss_{p,\infty}(J)$ and $ss_{p,3}(J)$ can be described as follows: let n_p be the degree of $ss_{p,3}(J)$. Then*

$$\frac{1}{ss_{p,\infty}(J)}\left(\frac{27}{64}J\right)^{n_p} ss_{p,3}\left(\frac{(4J-1)^3}{27J}\right) = \begin{cases} 1 & p \equiv 1 \ mod\ 12, \\ (J-1/4)^2 & p \equiv 5 \ mod\ 12, \\ (J+1/8) & p \equiv 7 \ mod\ 12, \\ (J-1/4)(J+1/8) & p \equiv 11 \ mod\ 12. \end{cases}$$

4.4.2. The non-arithmetic cases. In this section we prove some corollaries in the non-arithmetic setting, and consider one example from each of the cases $m \equiv 0 \bmod 4$, $m \equiv 2 \bmod 4$, and m odd.

First we state an analogue of Corollary 35 from the arithmetic setting.

COROLLARY 40. *The number of non-ordinary hyperelliptic curves over $\overline{\mathbb{F}}_p$ in the family $\mathcal{F}_m$ is finite (up to isogeny). The number of such curves is less than or equal to*

$$\sum_{i=1}^{\lceil g/2 \rceil} n_{p,i}.$$

The method of proof also makes apparent the following corollary, which more precisely examines the relationship between the roots of $\mathcal{P}_{m,p}$ and the genus of the curve C. In the statement we assume $b \neq 0$, but it is not difficult to modify the statements to consider the $b = 0$ case also.

Corollary 41. *Suppose $b \neq 0$. If J is a root of $\mathcal{P}_{m,j}$, then provided m is even or m is odd and J is not a root of $\mathcal{A}_{n_{p,i},m,k_{p,i}}$for $i = \frac{m+1}{2}$, the rank of the Hasse-Witt matrix is $g - 2m_J$, where m_J is the multiplicity of the root at J.*

If m is odd and J is a root of $\mathcal{A}_{n_{p,i},m,k_{p,i}}$ for $i = \frac{m+1}{2}$, the rank of the Hasse-Witt matrix is $g - 2m_J + 1$.

The slight discrepancy between the two cases highlighted in the previous corollary is best understood by exploring some examples.

Example 42. Consider the first non-arithmetic case, $m = 5$. In this case, the family of curves is given by the general hyperelliptic equation

$$y^2 = x\left(x^{10} - 2ax^5 + b\right).$$

Fix a prime, say $p = 41$, and consider such a curve over a field of characteristic p. Suppose also $b \neq 0$ so that the genus of this curve is 5. In this case,

$$\begin{aligned} u &= \left\lfloor \frac{41(2i-1)}{10} \right\rfloor, \\ j &= 41i - 20 - 5u, \end{aligned}$$

so that for $i = 1, 2, 3$, we have $j = i$. Therefore, the Hasse-Witt matrix is diagonal (in fact, this will be true whenever $p \equiv 1 \bmod 20$). Also, in all cases we have $\delta = \epsilon = 0$. By Lemma 33 and the proof of Theorem 4 if we denote the Hasse-Witt matrix by A, then

$$A = \begin{pmatrix} b^{16}\Delta^2\mathcal{A}_{2,5,2}(J) & & & & \\ & b^{28}\Delta^6\mathcal{A}_{6,5,1}(J) & & & \\ & & \Delta^{10}\mathcal{A}_{10,5,0}(J) & & \\ & & & \Delta^6\mathcal{A}_{6,5,1}(J) & \\ & & & & \Delta^2\mathcal{A}_{2,5,2}(J) \end{pmatrix},$$

where $\Delta = b - a^2$. From this we see the zeros along the diagonal are determined precisely by the zeros of the three Atkin-type polynomials $\mathcal{A}_{2,5,2}$, $\mathcal{A}_{6,5,1}$, and $\mathcal{A}_{10,5,0}$. Factoring these polynomials mod p, we find

$$\mathcal{A}_{2,5,2}(J) = J^2 + 36J + 30, \tag{4.4.3}$$

$$\mathcal{A}_{6,5,1}(J) = J^6 + 2J^5 + 12J^4 + 23J^3 + 9J^2 + 40J + 10, \tag{4.4.4}$$

$$\mathcal{A}_{10,5,0}(J) = (J+10)(J+16)(J+18)(J+37)(J^2+12J+10) \times(J^2+14J+1)(J^2+34J+37). \tag{4.4.5}$$

In particular, $\mathcal{A}_{6,5,1}$ is an irreducible degree 6 polynomial mod p; this contrasts with the arithmetic case, in which the Atkin polynomials always factor into products of irreducible factors of degree at most 2 over $\mathbb{F}_p$.

Meanwhile, if $b = 0$, the curve reduces to one of the form $y^2 = x^5 - 2a$. In this case, we see that the Hasse-Witt matrix reduces to

$$A = \begin{pmatrix} 10a^{12} & \\ & 30a^4 \end{pmatrix}$$

over a field of characteristic 41, and in particular always has full rank, since $a \neq 0$ if $b = 0$. Therefore, the case $b = 0$ never corresponds to a non-ordinary curve.

Because of this, and since the three Atkin-type polynomials above are pairwise coprime, the nonordinary polynomial coincides modulo 41 with $\mathcal{P}_{5,41}(J)$, which is just the product of these three Atkin-type polynomials. Consequently the nonordinary polynomial has degree 18.

We also see that the rank of the Hasse-Witt matrix is 5 if J is not a root of $\mathcal{P}_{5,41}$, equals 3 if J is a root of $\mathcal{A}_{2,5,2}$ or $\mathcal{A}_{6,5,1}$, and is 4 if J is a root of $\mathcal{A}_{10,5,0}$. This last case is only possible in general when m is odd, since when m is even g is even and Lemma 33 always gives a nontrivial symmetry between entries in the matrix.

Example 43. Consider the case $m = 10$. The corresponding curves are now of the form

$$y^2 = x^{10} - 2ax^5 + b$$

with $b - a^2 \neq 0$, and the genus of such a curve is 4 if $b \neq 0$ and 2 otherwise. This time we choose $p = 43$ and once again consider such a curve over the field of characteristic p. Suppose first that $b \neq 0$. Then the following table contains all relevant information in the two cases $i = 1$, $i = 2$:

i	j	u	n	k	δ	ϵ
1	3	8	5	1	0	1
2	1	17	9	3	1	0

From this, we see that the Hasse-Witt matrix in this case is equal to

$$A = \begin{pmatrix} & & b^{13}\Delta^4 \frac{\mathcal{A}_{5,10,1}(J)}{J} & \\ ab^4\Delta^8 \frac{\mathcal{A}_{9,10,3}(J)}{J-1} & & & \\ & & & a\Delta^8 \frac{\mathcal{A}_{9,10,3}(J)}{J-1} \\ & \Delta^4 \frac{\mathcal{A}_{5,10,1}(J)}{J} & & \end{pmatrix},$$

and modulo 43 we have

$$\begin{aligned} \mathcal{A}_{5,10,1}(J) &= J(J+16)(J^3+9J^2+27J+9), \\ \mathcal{A}_{9,10,3}(J) &= (J-1)(J+11)(J+19)(J^3+30J^2+13J+19) \\ &\quad \times(J^3+36J^2+28J+33). \end{aligned}$$

Notice that when $J = 1$, $a = 0$, so the entries of A in the second and fourth rows still vanish when $J = 1$ even though the factor of $J - 1$ is cancelled out of the Atkin-type polynomial. Related to this, when $b = 0$, the genus of the curve decreases by a factor of 2 and is birationally equivalent to a curve of the form

$$y^2 = x\left(x^5 - 2a\right).$$

In this case, $c_{ip-j} = 0$ for both values of j when $i = 2$, so we see the curve is always non-ordinary when $b = 0$. Therefore, even in this case, the $J = 0$ root of $\mathcal{A}_{5,10,1}(J)$ is detecting non-ordinariness of the curve.

As in the previous example, the relevant Atkin-type polynomials are coprime, and so we see the non-ordinary polynomial is simply the product of $\mathcal{A}_{5,10,1}$ and $\mathcal{A}_{9,10,3}$, and therefore has degree 14.

Example 44. For our last example we will consider the case $m = 12$. This gives rise to hyperelliptic curves of the form

$$y^2 = x\left(x^{12} - 2ax^6 + b\right)$$

of genus 6 provided $b \neq 0$ and $b - a^2 \neq 0$. As in the previous case we will set $p = 43$, and assume for the moment that b is nonzero. As i ranges from 1 to 3, the values of the other relevant parameters are captured in the following table:

i	j	u	n	k	δ	ϵ
1	4	3	3	1	1	1
2	5	10	6	3	0	1
3	6	17	10	5	1	1

This gives rise to the following Hasse-Witt matrix:

$$A = \begin{pmatrix} & & & ab^{18}\Delta\frac{\mathcal{A}_{3,12,1}(J)}{J(J-1)} & & \\ & & & & b^{11}\Delta^5\frac{\mathcal{A}_{6,4,1}(J)}{J} & \\ & & & & & ab^4\Delta^8\frac{\mathcal{A}_{10,12,5}(J)}{J(J-1)} \\ a\Delta^8\frac{\mathcal{A}_{10,12,5}(J)}{J(J-1)} & & & & & \\ & \Delta^5\frac{\mathcal{A}_{6,4,1}(J)}{J} & & & & \\ & & a\Delta\frac{\mathcal{A}_{3,12,1}(J)}{J(J-1)} & & & \end{pmatrix}.$$

Notice in this case that the second and fifth rows depend on an Atkin-type polynomial corresponding to $m = 4$, a proper divisor of 12. Indeed, since $\varphi(12)/2 = 2$, there are only two distinct J functions that can be obtained in the manner described in Chapter 2. In general, it is possible that the Hasse-Witt matrix may depend on Atkin-type polynomials indexed by proper divisors of m. In this case, the polynomial $\mathcal{A}_{6,4,1}(J)$ appears in the second row since when $i = 2$, $k = 3$, and we defined

$$\mathcal{A}_{n,m,k}(J) = \mathcal{A}_{n,\frac{m}{(m,k)},\frac{k}{(m,k)}}(J)$$

whenever k and m are not coprime.

Slightly different behavior also occurs when we look at the factorizations of the relevant Atkin-type polynomials modulo 43. Indeed, we have

$$\begin{aligned} \mathcal{A}_{3,12,1}(J) &= J(J-1)(J+19), \\ \mathcal{A}_{6,4,1}(J) &= J(J+5)(J+23)(J+34)(J^2+18J+6), \\ \mathcal{A}_{10,12,5}(J) &= J(J-1)(J+11)(J+19)(J^3+30J^2+13J+19)(J^3+36J^2+28J+33), \end{aligned}$$

and these polynomials are not pairwise coprime. In addition to the trivial common roots of $J = 0$ and $J = 1$ that occur whenever $\epsilon = 1$ and $\delta = 1$, respectively, there is also a nontrivial root $J + 19$ shared between $\mathcal{A}_{3,12,1}$ and $\mathcal{A}_{10,12,5}$.

If $b = 0$, and argument similar to the one in the previous example shows that $c_{ip-j} = 0$ for all values of j when $i = 1$, so once again the curve is always non-ordinary when $b = 0$. Therefore, in this case we see that the nonordinary polynomial is congruent to

$$\frac{\mathcal{P}_{12,43}(J)}{J^2(J-1)(J+19)},$$

and therefore is of degree 15.

Example 45. Our last example emphasizes the fact that the placement of the potential nonzero entries of the Hasse-Witt matrix depends only on the residue of p modulo $\frac{2m}{(2,m)}$. To see this, consider the example of $m = 8$. The family of curves is of the form

$$y^2 = x\left(x^8 - 2ax^4 + b\right)$$

and so when $b \neq 0$ and $b - a^2 \neq 0$ such a curve has genus 4.

For fixed $i \in \{1, 2\}$, we know that j is the unique integer between 1 and 4 such that

$$u = \frac{(2i-1)p - 2j + 1}{8} \in \mathbb{Z}.$$

In particular, the pairing of j values corresponding to the pair of i values depends only on the residue of p modulo 8. For example, when $p \equiv 1 \bmod 8$, $j = 1$ when $i = 1$ and $j = 2$ when $i = 2$. Denoting the four potential nonzero entries of the Hasse-Witt matrix by ν_1, ν_2, ν_3, and ν_4, it follows that the matrix is of one of the following forms:

$$\begin{pmatrix} \nu_1 & & & \\ & \nu_2 & & \\ & & \nu_3 & \\ & & & \nu_4 \end{pmatrix}, \begin{pmatrix} & \nu_1 & & \\ \nu_2 & & & \\ & & & \nu_3 \\ & & \nu_4 & \end{pmatrix},$$

$$\begin{pmatrix} & & \nu_1 & \\ & & & \nu_2 \\ \nu_3 & & & \\ & \nu_4 & & \end{pmatrix}, \begin{pmatrix} & & & \nu_1 \\ & & \nu_2 & \\ & \nu_3 & & \\ \nu_4 & & & \end{pmatrix},$$

depending on whether p is congruent to 1, 3, 5, or 7 modulo 8, respectively. The general case can be studied in a similar manner.

CHAPTER 5

Further applications

In this chapter, we highlight some further applications of the material discussed in previous chapters.

5.1. Connection to Jacobi polynomials

Recall that the Jacobi polynomial of degree n and depending on parameters α and β is given by

$$P_n^{(\alpha,\beta)}(x) = \frac{(\alpha+1)_n}{n!}\,{}_2F_1\left(-n, 1+\alpha+\beta+n; \alpha+1; \frac{1-x}{2}\right).$$

There are other equivalent definitions, but this one will be the most useful for our present purposes. We also note that for fixed α and β, the Jacobi polynomials are orthogonal with respect to the weight function

$$w_{\alpha,\beta}(x) = (1-x)^{\alpha}(1+x)^{\beta} \tag{5.1.1}$$

on $[-1,1]$. For more on Jacobi polynomials, see Chapter 4 of [35].

In [5], a connection is made between the supersingular polynomial for elliptic curves and certain Jacobi polynomials. While the authors do not discuss the Atkin polynomials, they do prove the following result, which provides a more elementary way to easily compute the supersingular polynomial for a fixed prime p.

Theorem 46. *For a prime $p > 3$, let $n = \left\lfloor \frac{p-1}{12} \right\rfloor$. Then*

$$ss_p(J) = J^{\epsilon}(J-1)^{\delta} P_n^{(\alpha,\beta)}(1-2J),$$

where α and β are given by

$$(\alpha,\beta) = \begin{cases} (-1/3,-1/2), & \text{if } p \equiv 1 \text{ mod } 12, \\ (1/3,-1/2), & \text{if } p \equiv 5 \text{ mod } 12, \\ (-1/3,1/2), & \text{if } p \equiv 7 \text{ mod } 12, \\ (1/3,1/2), & \text{if } p \equiv 12 \text{ mod } 12, \end{cases}$$

and

$$\epsilon = \begin{cases} 0 & \textit{if } p \equiv 1 \textit{ mod } 6, \\ 1 & \textit{if } p \equiv 5 \textit{ mod } 6, \end{cases}$$

$$\delta = \begin{cases} 0 & \textit{if } p \equiv 1 \textit{ mod } 4, \\ 1 & \textit{if } p \equiv 3 \textit{ mod } 4. \end{cases}$$

This is Theorem 3 of [5], though we have written it in a slightly different way here. In particular, we have written the supersingular polynomial in terms of J rather than the usual invariant $j = 1728J$. Notice that as an immediate corollary, we obtain the fact that the Atkin polynomial of degree $n_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \delta + \epsilon$ is essentially congruent mod p to a certain Jacobi polynomial.

The proof employed in [5] is somewhat technical, because the authors do not use Atkin polynomials. However, given what we know about generalized Atkin polynomials and their connection to hypergeometric functions, it is not difficult to prove an analogue of the above theorem in a more general setting.

The statement we wish to prove is the following:

THEOREM 47. *Let $m \geq 3$, and keep the notation as in Lemma 31. Then for a prime p not dividing $2m$, we have*

$$\mathcal{A}_{n_p,m,k}(J) = J^{\epsilon}(J-1)^{\delta} P^{(-1/2-u,\delta-1/2)}_{\left\lfloor \frac{u}{2} \right\rfloor}(1-2J)$$

over a field of characteristic p.

PROOF. First, notice that regardless of the value of m, over a field of characteristic p with $p \nmid 2m$ we can apply Lemma 31 and the definition of the truncated hypergeometric series $U^0_{n,m,k}$, $U^1_{n,m,k}$ to always write

$$\begin{aligned} \mathcal{A}_{n_p,m,k}(J) &= \mathcal{A}_{\left\lfloor \frac{u}{2} \right\rfloor + \delta + \epsilon, m, k} \\ &= U^{\delta}_{\left\lfloor \frac{u}{2} \right\rfloor + \delta + \epsilon, m, k}(J) \\ &= J^{\left\lfloor \frac{u}{2} \right\rfloor + \epsilon}(J-1)^{\delta} {}_2F_1\left(\alpha_{m,k} + \frac{\delta}{2}, \beta_{m,k} + \frac{\delta}{2}; 1; \frac{1}{J}\right). \end{aligned}$$

Note that $J^{\lfloor u/2 \rfloor} {}_2F_1\left(\alpha_{m,k} + \frac{\delta}{2}, \beta_{m,k} + \frac{\delta}{2}; 1; \frac{1}{J}\right)$ is always a polynomial of degree $\left\lfloor \frac{u}{2} \right\rfloor$, since p divides $\left\lfloor \frac{u}{2} \right\rfloor + \alpha_{m,k}$ when $\epsilon = \delta = 0$, p divides $\left\lfloor \frac{u}{2} \right\rfloor + \alpha_{m,k} + \frac{1}{2}$ when $\epsilon = 0$, $\delta = 1$, p divides $\left\lfloor \frac{u}{2} \right\rfloor + \beta_{m,k}$ when $\epsilon = 1$, $\delta = 0$, and p divides $\left\lfloor \frac{u}{2} \right\rfloor + \beta_{m,k} + \frac{1}{2}$ when $\epsilon = \delta = 1$.

By definition of the hypergeometric series, we see

$$\begin{aligned} J^{\left\lfloor \frac{u}{2} \right\rfloor} {}_2F_1\left(\alpha_{m,k}+\frac{\delta}{2},\beta_{m,k}+\frac{\delta}{2};1;\frac{1}{J}\right) &= \sum_{\ell=0}^{\left\lfloor \frac{u}{2} \right\rfloor} \frac{\left(\alpha_{m,k}+\frac{\delta}{2}\right)_\ell \left(\beta_{m,k}+\frac{\delta}{2}\right)_\ell}{\ell!^2} J^{\left\lfloor \frac{u}{2} \right\rfloor-\ell} \\ &= \sum_{\ell=0}^{\left\lfloor \frac{u}{2} \right\rfloor} \frac{\left(\alpha_{m,k}+\frac{\delta}{2}\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell} \left(\beta_{m,k}+\frac{\delta}{2}\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell}}{\left(\left\lfloor \frac{u}{2} \right\rfloor-\ell\right)!^2} J^\ell. \end{aligned}$$

Also, regardless of the value of m we see by definition of k that $-\frac{u}{2}$ is congruent to either $\alpha_{m,k}$ or $\beta_{m,k}$ mod p. Since $\alpha_{m,k}+\beta_{m,k}=\frac{1}{2}$, in either case we may rewrite the above sum as

$$\begin{aligned} &\sum_{\ell=0}^{\left\lfloor \frac{u}{2} \right\rfloor} \frac{\left(\frac{\delta-u}{2}\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell} \left(\frac{1+u+\delta}{2}\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell}}{\left(\left\lfloor \frac{u}{2} \right\rfloor-\ell\right)!^2} J^\ell \\ = &\sum_{\ell=0}^{\left\lfloor \frac{u}{2} \right\rfloor} \frac{\left(-\left\lfloor \frac{u}{2} \right\rfloor\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell} \left(\frac{1}{2}+u-\left\lfloor \frac{u}{2} \right\rfloor\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell}}{\left(\left\lfloor \frac{u}{2} \right\rfloor-\ell\right)!^2} J^\ell, \end{aligned}$$

since $\delta = u - 2\left\lfloor u/2 \right\rfloor$.

Denote the above coefficient on J^ℓ by c_ℓ. By definition of the Pochhammer symbol, we can rewrite c_ℓ as

$$\begin{aligned} c_\ell &= \frac{\left\lfloor \frac{u}{2} \right\rfloor! \left(-\left\lfloor \frac{u}{2} \right\rfloor+u+\frac{1}{2}\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell} (-1)^{\left\lfloor \frac{u}{2} \right\rfloor-\ell}}{\left(\left\lfloor \frac{u}{2} \right\rfloor-\ell\right)!^2 \ell!} \\ &= \frac{\left\lfloor \frac{u}{2} \right\rfloor! \left(\frac{1}{2}-u+\ell\right)_{\left\lfloor \frac{u}{2} \right\rfloor-\ell}}{\left(\left\lfloor \frac{u}{2} \right\rfloor-\ell\right)!^2 \ell!}. \end{aligned}$$

In particular,

$$c_0 = \frac{\left(\frac{1}{2}-u\right)_{\left\lfloor \frac{u}{2} \right\rfloor}}{\left\lfloor \frac{u}{2} \right\rfloor!}.$$

The numerator here is never divisible by p. One way to see this is to note that if p divides one of the factors in the numerator, then we must have $1-2u+k \equiv 0 \bmod p$ for some k between 0 and $\left\lfloor \frac{u}{2} \right\rfloor - 1$. But regardless of m, we always have that $2u < p$, so that such a congruence cannot hold.

We now show that for $0 \leq \ell \leq \left\lfloor \frac{u}{2} \right\rfloor$,

$$c_\ell = c_0 \frac{\left(-\left\lfloor \frac{u}{2} \right\rfloor\right)_\ell^2}{\ell! \left(\frac{1}{2}-u\right)_\ell}. \tag{5.1.2}$$

This expression always makes sense since we have just seen that the denominator is never congruent to 0 mod p.

When $\ell = 0$ there is nothing to prove. If the result holds for c_ℓ, then

$$\begin{aligned} c_{\ell+1} &= \frac{\left\lfloor \frac{u}{2} \right\rfloor! \left(\frac{1}{2} - u + \ell + 1\right)_{\left\lfloor \frac{u}{2} \right\rfloor - \ell - 1}}{\left(\left\lfloor \frac{u}{2} \right\rfloor - \ell - 1\right)!^2 \, (\ell+1)!} \\ &= c_\ell \frac{\left(\ell - \left\lfloor \frac{u}{2} \right\rfloor\right)^2}{(\ell+1)\left(\frac{1}{2} - u + \ell\right)} \\ &= c_0 \frac{\left(-\left\lfloor \frac{u}{2} \right\rfloor\right)_{\ell+1}^2}{(\ell+1)!\left(\frac{1}{2} - u\right)_{\ell+1}}, \end{aligned}$$

where we have used the induction hypothesis in the last step. Therefore (5.1.2) holds by induction.

Putting everything together,

$$\begin{aligned} \mathcal{A}_{n_p,m,k}(J) &= J^\epsilon (J-1)^\delta \sum_{\ell=0}^{\lfloor u/2 \rfloor} c_\ell J^\ell \\ &= J^\epsilon (J-1)^\delta \frac{\left(\frac{1}{2} - u\right)_{\lfloor u/2 \rfloor}}{\lfloor u/2 \rfloor!} \sum_{\ell=0}^{\lfloor u/2 \rfloor} \frac{\left(-\left\lfloor \frac{u}{2} \right\rfloor\right)_\ell^2}{\ell! \left(\frac{1}{2} - u\right)_\ell} J^\ell \\ &= J^\epsilon (J-1)^\delta \frac{\left(\frac{1}{2} - u\right)_{\lfloor u/2 \rfloor}}{\lfloor u/2 \rfloor!} {}_2F_1\left(-\left\lfloor \frac{u}{2} \right\rfloor, -\left\lfloor \frac{u}{2} \right\rfloor; \frac{1}{2} - u; J\right). \end{aligned}$$

Setting α equal to $-1/2 - u$ then determines β as $\delta - 1/2$ via the equality

$$1 + \alpha + \beta + \left\lfloor \frac{u}{2} \right\rfloor = -\left\lfloor \frac{u}{2} \right\rfloor,$$

and with these choices, we see that the above expression becomes simply

$$J^\epsilon (J-1)^\delta P_{\left\lfloor \frac{u}{2} \right\rfloor}^{(-1/2-u, \delta-1/2)}(1 - 2J).$$

This completes the proof. □

Some remarks are in order. First, note that for fixed m and p, the above result only applies to a specific generalized Atkin polynomial of some fixed degree, not to every generalized Atkin polynomial in the family. Moreover, the statement only holds over a field of characteristic p. By way of example, note that if we return to the case $m = 5$, $p = 41$ from the previous chapter, we obtain three generalized Atkin polynomials corresponding to the values $i = 1, 2, 3$. Recall that in each case, $\epsilon = \delta = 0$ and $i = j$. Therefore, since

$$u = \frac{(2i-1)p - 2j + 1}{2m},$$

we see that $u = 4, 12$, or 20, according to the value of i.

When $i = 1$, the relevant Atkin polynomial is

$$\mathcal{A}_{2,5,2}(J) = J^2 - \frac{581}{600}J + \frac{1653}{16000},$$

while the relevant Jacobi polynomial is

$$P_2^{\left(-\frac{9}{2},-\frac{1}{2}\right)}(1-2J) = J^2 - 5J + \frac{35}{8}.$$

Both polynomials, however, are equivalent modulo 41 to (4.4.3).

Similarly, when $i = 2$, the relevant Atkin polynomial is

$$\begin{aligned}\mathcal{A}_{6,5,1}(J) \quad = \quad & J^6 - \frac{1293}{440}J^5 + \frac{28281339}{8800000}J^4 - \frac{8441564927}{5280000000}J^3 + \frac{1147233310111}{3276800000000}J^2 \\ & -\frac{427439820336993}{16384000000000000}J + \frac{237875498609889}{131072000000000000},\end{aligned}$$

which is much messier than the relevant Jacobi polynomial

$$\begin{aligned}P_6^{\left(-\frac{25}{2},-\frac{1}{2}\right)}(1-2J) \quad = \quad & J^6 - 39J^5 + \frac{2925}{8}J^4 - \frac{5525}{4}J^3 \\ + \quad & \frac{314925}{128}J^2 - \frac{264537}{128}J + \frac{676039}{1024}.\end{aligned}$$

Both, however, are congruent modulo 41 to (4.4.4).

Lastly, when $i = 3$, the relevant Atkin polynomial is

$$\begin{aligned}\mathcal{A}_{10,5,0}(J) \quad = \quad & J^{10} - \frac{749}{152}J^9 + \frac{9385}{912}J^8 - \frac{11761043}{992256}J^7 + \frac{44473367407}{5419040768}J^6 \\ - \quad & \frac{23890048637}{6845104128}J^5 + \frac{218583737141}{244813135872}J^4 - \frac{1426583125165}{11098195492864}J^3 \\ + \quad & \frac{1229793398431339}{136374626216312832}J^2 - \frac{238475774882381}{1090997009730502656}J + \frac{4418157975}{18014398509481984}.\end{aligned}$$

The corresponding Jacobi polynomial becomes

$$\begin{aligned}P_{10}^{\left(-\frac{41}{2},-\frac{1}{2}\right)}(J) \quad = \quad & J^{10} - 105J^9 + \frac{21735}{8}J^8 - \frac{60375}{2}J^7 + \frac{11410875}{64}J^6 \\ - \quad & \frac{39709845}{64}J^5 + \frac{683891775}{512}J^4 - \frac{460580175}{256}J^3 \\ + \quad & \frac{48360918375}{32768}J^2 - \frac{22090789875}{32768}J + \frac{34461632205}{262144},\end{aligned}$$

and both are congruent modulo 41 to (4.4.5).

Also, notice that the values of α are growing larger with u. However, since we only consider u modulo p, it is possible to find smaller values of α that will also provide us with a suitable equivalence. In the above example, for instance, we have that

$$u = \frac{41(2i-1)-2j+1}{10} \equiv \frac{-2j+1}{10} \bmod 41.$$

Therefore, instead of the values $\alpha = -9/2, -25/2, -41/2$ considered above, we could just as easily have taken $\alpha = -\frac{2}{5}, -\frac{1}{5}$, and 0, respectively (corresponding to the cases $j=1, j=2, j=3$). This would give rise to the Jacobi polynomials

$$\begin{aligned}
P_2^{\left(-\frac{2}{5},-\frac{1}{2}\right)}(1-2J) &= \frac{651}{200}J^2 - \frac{84}{25}J + \frac{12}{25}, \\
P_6^{\left(-\frac{1}{5},-\frac{1}{2}\right)}(1-2J) &= \frac{45908976351}{80000000}J^6 - \frac{35345849049}{20000000}J^5 + \frac{1029490749}{500000}J^4 \\
&- \frac{70108689}{62500}J^3 + \frac{17738343}{62500}J^2 - \frac{2186919}{78125}J + \frac{46284}{78125}, \\
P_{10}^{\left(0,-\frac{1}{2}\right)}(1-2J) &= \frac{34461632205}{262144}J^{10} - \frac{22090789875}{32768}J^9 + \frac{48360918375}{32768}J^8 \\
&- \frac{460580175}{256}J^7 + \frac{683891775}{512}J^6 - \frac{39709845}{64}J^5 \\
&+ \frac{11410875}{64}J^4 - \frac{60375}{2}J^3 + \frac{21735}{8}J^2 - 105J + 1,
\end{aligned}$$

and these are again congruent to (4.4.3), (4.4.4), and (4.4.5) mod 41, respectively.

These latter choices of α are more in line with the α seen in Theorem 46. By considering the separate cases of m individually, we can therefore modify the statement of Theorem 47 so that it more readily agrees with the statement of Theorem 46. We give this new statement as a corollary.

COROLLARY 48. *Let $m \geq 3$, and keep the notation as in Lemma 31. Then for a prime p not dividing $2m$, we have the following:*

(i) if $m \equiv 0$ mod 4, then for $1 \leq i \leq \frac{m}{4}$ and j satisfying $\frac{(2i-1)p+1}{2} \equiv j$ mod $m/2$, we have

$$\mathcal{A}_{n_p,m,k}(J) = J^{\epsilon}(J-1)^{\delta} P_{\left\lfloor \frac{(2i-1)p}{2m} \right\rfloor}^{\left(-\frac{1}{2}+\frac{2j-1}{m},\delta-\frac{1}{2}\right)}(1-2J)$$

over a field of characteristic p.

(ii) if $m \equiv 2$ mod 4, then for $1 \leq i \leq \frac{m-2}{4}$ and j satisfying $j \equiv ip$ mod $m/2$, we have

$$\mathcal{A}_{n_p,m,k}(J) = J^{\epsilon}(J-1)^{\delta} P_{\left\lfloor \frac{ip}{m} \right\rfloor}^{\left(-\frac{1}{2}+\frac{j}{m/2},\delta-\frac{1}{2}\right)}(1-2J)$$

over a field of characteristic p.

(iii) if m is odd, then for $1 \leq i \leq \frac{m+1}{2}$ and j satsifying $\frac{(2i-1)p+1}{2} \equiv j$ mod m, we have

$$\mathcal{A}_{n_p,m,k}(J) = J^{\epsilon}(J-1)^{\delta} P_{\left\lfloor \frac{(2i-1)p}{4m} \right\rfloor}^{\left(-\frac{1}{2}+\frac{2j-1}{2m},\delta-\frac{1}{2}\right)}(1-2J)$$

over a field of characteristic p.

5.2. Jacobians of the curves in $\mathcal{F}_m$

In the arithmetic cases $m = 4$ and $m = 6$, it is known that the Jacobian of a curve in $\mathcal{F}_m$ with $b \neq 0$ is isogenous to a product of elliptic curves over $\mathbb{C}$; moreover, these elliptic curves are themselves isogenous (see the remarks in [9], for example). Over a finite field, one obtains a similar splitting of the Jacobian, though one may need to pass to a field extension to obtain an isogeny between the two elliptic curves (see [63, 24]).

Based on these observations, it is natural to ask whether any sort of splitting of the Jacobian occurs in general for the curves in $\mathcal{F}_m$. In this section, we show that the Jacobian of a curve in $\mathcal{F}_m$ with $b \neq 0$ is always isogenous over $\mathbb{C}$ to a product of Jacobians of lower genus hyperelliptic curves. While we restrict to the case $b \neq 0$, similar arguments could be used to treat the $b = 0$ case.

Since we are working over $\mathbb{C}$, to simplify the notation a bit, we begin by transforming the equation

$$y^2 = x^{2g+1+\kappa_m} - 2ax^{g+1} + bx^{1-\kappa_m}$$

of a curve in $\mathcal{F}_m$ with $b = 0$ to the form

$$y^2 = x^{2g+1+\kappa_m} - \theta x^{g+1} + x^{1-\kappa_m} \tag{5.2.1}$$

via the mapping

$$\begin{aligned} y/b^{1/2} &\mapsto y, \\ x/b^{\frac{1}{2g+1+\kappa_m}} &\mapsto x, \end{aligned}$$

where

$$\theta = \frac{2a}{b^{\frac{g+\kappa_m}{2g+1+\kappa_m}}}.$$

With this notation, we prove the following result.

Theorem 49. *Let C be a curve in $\mathcal{F}_m$ of the form (5.2.1).*

(i) If m is even, then the Jacobian of C is isogenous to $\mathcal{J}_0 \times \mathcal{J}_1$, where $\mathcal{J}_j$ is the Jacobian of the hyperelliptic curve

$$C_j : Y^2 = X\left(-\theta + \sum_{k=0}^{m/2} (-1)^{(1-j)k} a_{k,m} X^{m/2-k}\right),$$

and

$$a_{k,m} = \frac{m\,(m-k-1)!}{k!\,(m-2k)!}.$$

(ii) If m is odd, then the Jacobian of C is isogenous to $\mathcal{J}_0 \times \mathcal{J}_1 \times E_\theta$, where $\mathcal{J}_j$ is the Jacobian of the hyperelliptic curve

$$C_j : Y^2 = -\theta + \sum_{k=0}^{\frac{m-1}{2}} (-1)^k \zeta_m^{-2jk} a_{k,m} X^{m-2k},$$

ζ_m is a fixed nontrivial mth root of unity, and E_θ is the elliptic curve

$$Y^2 = X^3 + \left(1 - \frac{\theta^2}{3}\right) X + \frac{\theta}{3}\left(1 - \frac{2\theta^2}{9}\right). \tag{5.2.2}$$

In particular, E_θ is independent of m.

Proof. Our method of proof is a generalization of the proof given in [48] for the case $m = 4$. We focus first on the case where m is even. In this case, $g = m/2 - \kappa_m$ and the right hand side of (5.2.1) reduces to

$$\begin{aligned} & x^{1-\kappa_m}\left(x^m - \theta x^{m/2} + 1\right) \\ = \;& x^{g+1}\left(x^{m/2} + x^{-m/2} - \theta\right). \end{aligned}$$

For $j \in \{0, 1\}$, consider the transformation

$$\begin{aligned} \varphi_j(x, y) &= \left(\frac{\left(x + (-1)^j\right)^2}{x}, \frac{y\left(x + (-1)^j\right)}{x^{g/2+1}} \right) \\ &= (X, Y). \end{aligned}$$

In particular, $X = x + x^{-1} \pm 2$, with the sign being positive for $j = 0$ and negative for $j = 1$. In other words, $X + 2(-1)^{1-j} = x + x^{-1}$.

The idea is to use the well known expression of $x^n + x^{-n}$ as a polynomial in $x + x^{-1}$. This polynomial is closely related to the Chebyshev polynomial

$$T_n(t) = \frac{\left(t - \sqrt{t^2 - 1}\right)^n + \left(t + \sqrt{t^2 - 1}\right)^n}{2}.$$

In particular, for $t = \frac{x + x^{-1}}{2}$,

$$x^n + x^{-n} = 2T_n\left(\frac{x + x^{-1}}{2}\right),$$

and in fact

$$x^n + x^{-n} = 2T_n\left(\frac{x\zeta_n^{-1} + x^{-1}\zeta_n}{2}\right) \tag{5.2.3}$$

for any nth root of unity ζ_n. Using this identity,

$$Y^2 = X\left(2T_{m/2}\left(\frac{X}{2} + (-1)^{1-j}\right) - \theta\right). \tag{5.2.4}$$

We now list the following well-known properties of the polynomial T_n :

$$\begin{aligned} T_n\left(1-2x^2\right) &= (-1)^n\, T_{2n}(x), & (5.2.5)\\ T_n(x) &= {}_2F_1\left(-n, n; \frac{1}{2}; \frac{1-x}{2}\right) & \\ &= \frac{n}{2}\sum_{k=0}^{\lfloor n/2\rfloor} (-1)^k\, \frac{(n-k-1)!}{k!\,(n-2k)!}\,(2x)^{n-2k}. & (5.2.6)\end{aligned}$$

By combining these properties, we see that when $j = 0$,

$$\begin{aligned} 2T_{m/2}\left(\frac{X}{2} - 1\right) &= 2T_m\left(\frac{X^{1/2}}{2}\right) \\ &= m\sum_{k=0}^{m/2} (-1)^k\, \frac{(m-k-1)!}{k!\,(m-2k)!} X^{m/2-k}, \end{aligned}$$

so that (5.2.4) reduces to the equation for C_0. Similarly, when $j = 1$,

$$\begin{aligned} 2T_{m/2}\left(\frac{X}{2} + 1\right) &= 2(-1)^{m/2} T_m\left(\frac{iX^{1/2}}{2}\right) \\ &= m\sum_{k=0}^{m/2} \frac{(m-k-1)!}{k!\,(m-2k)!} X^{m/2-k}, \end{aligned}$$

so that (5.2.4) reduces to the equation for C_1.

We still need to show that the Jacobian of our original curve is isogenous to the product $\mathcal{J}_0 \times \mathcal{J}_1$. To see why this is so, for $0 \le \ell < g$, let

$$\omega_\ell = x^\ell \frac{dx}{y}.$$

These differentials form a well known basis of the space of holomorphic differentials for the curve C. Also, for $0 \le s < g/2$, let

$$\omega_{j,s} = X^s \frac{dX}{Y}$$

denote the basis elements for the space of holomorphic differentials for the curve C_j. By direct computation, we see

$$\begin{aligned} X^s \frac{dX}{Y} &= (x+1)^{2s}\,(x-1)\,x^{g/2-1-s}\frac{dx}{y} \\ &= \sum_{r=0}^{2s} \binom{2s}{r} x^{r+g/2-1-s}\,(x-1)\,\frac{dx}{y}, \end{aligned}$$

so that

$$\varphi_1^*\left(\omega_{1,s}\right) = \sum_{r=-1}^{2s} c(r,2s)\omega_{r+g/2-s},$$

where

$$\begin{aligned} c(r,s) &= \binom{s}{r} - \binom{s}{r+1} \\ &= \frac{2r+1-s}{r+1}\binom{s}{r}. \end{aligned} \tag{5.2.7}$$

In particular, $c(r,2s) \neq 0$ since $2s$ is always even. Similarly, we find that

$$\varphi_0^*\left(\omega_{0,s}\right) = \sum_{r=-1}^{2s} (-1)^r c(r,2s)\omega_{r+g/2-s},$$

so that in general

$$\varphi_j^*\left(\omega_{j,s}\right) = \sum_{r=-1}^{2s} (-1)^{r(1-j)} c(r,2s)\omega_{r+g/2-s}.$$

If we now consider the g dimensional column vectors

$$\begin{aligned} v &= \left(\varphi_1^*\left(\omega_{1,0}\right), \varphi_0^*\left(\omega_{0,0}\right), \dots, \varphi_1^*\left(\omega_{1,s}\right), \varphi_0^*\left(\omega_{0,s}\right) \dots, \varphi_1^*\left(\omega_{1,\frac{g}{2}-1}\right), \varphi_0^*\left(\omega_{0,\frac{g}{2}-1}\right)\right), \\ w &= \left(\omega_{\frac{g}{2}-1}, \omega_{\frac{g}{2}}, \dots, \omega_{\frac{g}{2}-\ell-1}, \omega_{\frac{g}{2}+\ell}, \dots, \omega_0, \omega_{g-1}\right), \end{aligned}$$

then the matrix A satisfying

$$Aw = v$$

is a block lower triangular matrix of the form

$$\begin{pmatrix} A_0 & & & 0 \\ & A_1 & & \\ & & \ddots & \\ * & & & A_{g/2-1} \end{pmatrix},$$

where each A_s is a 2×2 matrix of the form

$$A_s = \begin{pmatrix} c(-1,2s) & c(2s,2s) \\ -c(-1,2s) & c(2s,2s) \end{pmatrix}.$$

In particular, each A_i has nonzero determinant since we have already observed that the values of $c(r,2s)$ are nonzero. Therefore A has full rank, and so the forms $\varphi_j^*\left(\omega_{j,s}\right)$ for $0 \leq j \leq 1$ and $0 \leq s \leq g/2-1$ also form a basis for the space of holomorphic differential forms on C. This proves the desired isogeny holds (in fact, over $\mathbb{Q}(\theta)$).

Let us now consider the case of m odd. The main argument is the same, though there are some important differences. A curve in $\mathcal{F}_m$ is now of the form

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

The first thing to notice is that if we set

$$X = x + x^{-1} \pm 2$$

as in the previous case, the corresponding value of Y becomes

$$Y = y/x^{\frac{m+1}{2}},$$

and consequently, using notation analogous to the previous case,

$$\varphi_0^*\left(\omega_{0,0}\right) = \varphi_1^*\left(\omega_{1,0}\right).$$

In particular, the differentials one obtains from this transformation do not form a spanning set. Therefore, we need to choose our transformation somewhat more carefully. One way to do this is to fix an mth root of unity ζ_m, and apply (5.2.3) to rewrite the right hand side of the equation defining our curve as

$$\begin{aligned} x\left(x^{2m} - \theta x^m + 1\right) &= x^{m+1}\left(x^m + x^{-m} - \theta\right) \\ &= x^{m+1}\left(2T_m\left(\frac{x\zeta_m^{-j} + x^{-1}\zeta_m^{j}}{2}\right) - \theta\right) \end{aligned}$$

for $j = 0, 1$. Now if we set

$$\begin{aligned} \varphi_j(x, y) &= \left(x + \frac{\zeta_m^2}{x}, \frac{y}{x^{\frac{m+1}{2}}}\right) \\ &= (X, Y), \end{aligned}$$

our original curve becomes

$$\begin{aligned} Y^2 &= 2T_m\left(\frac{\zeta_m^{-j} X}{2}\right) - \theta \\ &= -\theta + m\sum_{k=0}^{\frac{m-1}{2}} (-1)^k \zeta_m^{-2kj} \frac{(m-k-1)!}{k!\,(m-2k)!} X^{m-2k}, \end{aligned}$$

and we therefore obtain the curves C_j.

We next compute some differentials. Keeping the same notation from the previous case, we have

$$\begin{aligned}\varphi_j^*\left(\omega_{j,s}\right) &= \left(\frac{x^2+\zeta_m^{2j}}{x}\right)^s\left(\frac{1-x^{-2}\zeta_m^{2j}}{y}\right)x^{\frac{m+1}{2}}\frac{dx}{y}\\ &= \sum_{r=0}^{s}\binom{s}{r}\zeta_m^{2j(s-r)}x^{\frac{m-3}{2}-s}\left(x^2-\zeta_m^{2j}\right)\frac{dx}{y}\\ &= \sum_{r=-1}^{s}c(r,s)\zeta_m^{2j(s-r)}\omega_{2r+\frac{m+1}{2}-s}.\end{aligned}$$

Here $c(r,s)$ is once again given by (5.2.7). Notice that we still have to worry about spanning, since in this case we have $c(r,s)=0$ whenever $r=\frac{s-1}{2}$. In particular, the coefficient of $\omega_{\frac{m-1}{2}}$ is always zero.

Ignoring this form for the time being, we can try to proceed as in the previous case. If we consider the $m-1$ dimensional vectors

$$\begin{aligned}v &= \left(\varphi_1^*\left(\omega_{1,0}\right),\varphi_0^*\left(\omega_{0,0}\right),\ldots,\varphi_1^*\left(\omega_{1,s}\right),\varphi_0^*\left(\omega_{0,s}\right)\ldots,\varphi_1^*\left(\omega_{1,\frac{m-3}{2}}\right),\varphi_0^*\left(\omega_{0,\frac{m-3}{2}}\right)\right),\\ w &= \left(\omega_{\frac{m-3}{2}},\omega_{\frac{m+1}{2}},\ldots,\omega_{\frac{m-1}{2}-\ell-1},\omega_{\frac{m+1}{2}+\ell},\ldots,\omega_0,\omega_{m-1}\right),\end{aligned}$$

then the matrix A satisfying

$$Aw=v$$

is once again a block lower triangular matrix, this time of dimension $(m-1)\times(m-1)$, and of the form

$$\begin{pmatrix} A_0 & & & 0\\ & A_1 & & \\ & & \ddots & \\ * & & & A_{\frac{m-3}{2}}\end{pmatrix},$$

where each A_s is a 2×2 matrix of the form

$$A_s=\begin{pmatrix}\zeta_m^{2(s+1)}c(-1,s) & c(s,s)\\ c(-1,s) & c(s,s)\end{pmatrix}.$$

Since $c(-1,s)$ and $c(s,s)$ are both nonzero, and since $s<\frac{m-1}{2}$, we see that $\det A_s\neq 0$ for each s, so that this matrix has full rank. Therefore the forms $\varphi_j^*\left(\omega_{j,s}\right)$ for $0\le j\le 1$ and $0\le s\le\frac{m-3}{2}$ form a basis for the subspace of holomorphic differential forms for C spanned by ω_ℓ for $\ell\neq\frac{m-1}{2}$.

To cover this last basis element, we need one final transformation. If we start again with the curve

$$C: y^2=x\left(x^{2m}-\theta x^m+1\right),$$

then clearly

$$\begin{aligned}\left(x^{\frac{m-1}{2}}y\right)^2 &= x^{3m}-\theta x^{2m}+x^m \\ &= \left(x^m-\frac{\theta}{3}\right)^3+x^m\left(1-\frac{\theta^2}{3}\right)+\frac{\theta^3}{27}.\end{aligned}$$

Therefore, if we set

$$\begin{aligned}\varphi_\theta\left(x,y\right) &= \left(x^m-\frac{\theta}{3},x^{\frac{m-1}{2}}y\right) \\ &= \left(X,Y\right),\end{aligned}$$

then X and Y satisfy the equation (5.2.2) of the curve E_θ. In this case, we see

$$\frac{dX}{Y}=mx^{\frac{m-1}{2}}\frac{dx}{y},$$

or in other words,

$$\varphi_\theta^*\left(\omega_\theta\right)=m\omega_{\frac{m-1}{2}},$$

where $\omega_\theta=dX/Y$. We conclude that the forms $\varphi_j^*\left(\omega_{j,s}\right)$ along with the form $\varphi_\theta^*\left(\omega_\theta\right)$ form a basis for the space of holomorphic differential forms for C, and therefore the isogeny holds (this time over $\mathbb{Q}\left(\theta,\zeta_m^2\right)$). □

We close this section with some remarks. First, it's quite likely that the above result could be strengthened. For example, in [16] it is shown in the case $m\equiv 2 \bmod 4$ that the Jacobian of C is actually isomorphic to a product of Jacobians. It's possible one could extend this result to the more general setting studied here.

Second, it is instructive to treat the $m=3$ case in this context. Of course, this case has already been described in detail, but it is possible for some confusion to arise, since the $m=3$ case deals with elliptic curves, but in this more general framework, the family $\mathcal{F}_3$ is given by hyperelliptic curves of the form

$$y^2=x\left(x^6-ax^3+b\right).$$

To reconcile this apparent discrepancy, we know by the theorem above that the Jacobian splits into $E_0\times E_1\times E_\theta$, for some elliptic curves E_0 and E_1, where E_θ is given by (5.2.2). Using the notation of the above theorem, we see that for $j=0,1$, E_j is given by

$$Y^2=X^3-\zeta_3^{-2j}X-\theta,$$

and in particular these curves are isomorphic, since the mapping

$$\left(X,Y\right)\mapsto\left(\zeta_3X,Y\right)$$

takes E_0 to E_1. Therefore the Jacobian splits into $E_0^2 \times E_\theta$.

For $m = 3$, the dependence of θ on a and b is given by

$$\theta = \frac{2a}{b^{1/2}}.$$

It follows that the j invariant of the curve E_0 is equal to

$$1728\frac{4}{4-\theta^2} = 1728\frac{b}{b-a^2}.$$

Therefore, the results on supersingular elliptic curves and Atkin polynomials discussed, for example, in [40], can be obtained from analysis of the curves in $\mathcal{F}_3$ by looking at the factor E_0 in the Jacobian of the curve.

5.3. Period functions and modular integrals

5.3.1. Background on Modular Integrals for G_3. There is another way to interpret the Atkin polynomials and their generalizations. This approach makes use of the theory of period functions and modular integrals.

Let us first recall some of the terminology in the case of the full modular group $G_3 = PSL_2(\mathbb{Z})$. Let S and $T = T_3$ denote the generators of this group, as introduced in the first chapter, and let $U = ST$. A holomorphic function ψ on $\mathbb{H}$ is said to be a period function of even integral weight k if it satisfies the functional equations

$$\psi \mid_k (1+S) = 0, \tag{5.3.1}$$

$$\psi \mid_k \left(1+U+U^2\right) = 0, \tag{5.3.2}$$

along with the growth condition

$$|\psi(\tau)| \ll |\tau|^A + \mathrm{Im}\,(\tau)^{-B}$$

for some positive constants A and B and some even integer k, where

$$\psi \mid_k g(\tau) = (cz+d)^{-k}\,\psi\,(g\tau)$$

denotes the usual slash operator for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$.

Now consider a holomorphic function F on $\mathbb{H}$ which has a q-series expansion ($q = e^{2\pi i\tau}$)

$$F(\tau) = \sum_n a(n)q^n,$$

and let $\mathrm{ord}_\infty F \in \mathbb{Z} \cup \{\pm\infty\}$ denote the smallest n for which $a(n) \neq 0$. If such an F satisfies $\mathrm{ord}_\infty F > -\infty$ and

$$F \mid_k (1 - S) = \psi,$$

for some period function ψ of weight k, then F is called a modular integral of weight k for G_3 and ψ.

Example 50. Consider the weight 2 Eisenstein series E_2 for the full modular group. Because of the transformation property (2.1.1),

$$E_2 \mid_2 (1 - S)(\tau) = \frac{6i}{\pi\tau},$$

so that E_2 is a modular integral for G_3 with period function $\frac{6i}{\pi\tau}$ (for the statement that $1/\tau$ is a period function, see Proposition 52 below).

The mapping from a modular integral F to its corresponding period function ψ is linear, and the kernel of this map defines the space of weakly holomorphic modular forms of weight k, typically denoted $M_k^!$. These functions satisfy the same functional equations as modular forms, but we allow for poles at the cusp $i\infty$. As explained in [15], if we write the weight k as $k = 12\ell + k'$ for $k \in \{0, 4, 6, 8, 10, 14\}$, then

$$\ell = \begin{cases} \lfloor k/12 \rfloor - 1, & k \equiv 2 \text{ mod} 12, \\ \lfloor k/12 \rfloor, & \text{otherwise} \end{cases}$$

is the dimension of the space of cusp forms of even weight k when $k > 2$, and consequently by the Riemann-Roch theorem for each $m \geq -\ell$ there exists a weakly holomorphic modular form of weight k, denoted $f_{k,m}$, of the form

$$f_{k,m}(\tau) = q^{-m} + \sum_{n > \ell} a_k(m, n) q^n.$$

In fact, we can write the function $f_{k,m}$ as

$$f_{k,m} = \Delta^\ell E_{k'} P_{k,m}(j),$$

where Δ denotes the canoncal cusp form of weight 12, $E_{k'}$ is the weight k' Eisenstein series, and $P_{k,m}(j)$ is a monic polynomial of degree $m + \ell$ in the modular invariant $j = 1728 J_3$. More on these polynomials, sometimes referred to as a type of generalized Faber polynomial, can be found in [37]. Note in particular, when $m = -\ell$ we have $f_{k,-\ell} = f_k = \Delta^\ell E_{k'}$.

While it might not seem obvious that one can always find a modular integral for a given period function ψ, Knopp showed in [41] that the linear mapping from modular integrals to period functions is surjective. If we impose the additional restriction that $\mathrm{ord}_\infty F > \ell$ for ℓ as above, then in fact Knopp's construction can be used to give rise to a *unique* modular integral associated to ψ, which we will denote by F_ψ.

Though the integral F_ψ can be difficult to compute explicitly, in certain cases such computations are possible. For example, if $k > 2$ then for each $m \geq -\ell$, $m \neq 0$, there exists a modular integral called the Eichler integral associated to the weakly holomorphic modular form $f_{k,m}$ and defined by

$$F_{k,m}(\tau) = (-m)^{1-k} q^{-m} + \sum_{n>\ell} a_k(m,n) n^{1-k} q^n.$$

This is a modular integral of weight $2-k$ and is associated to a period function $\psi_{k,m}$ which is a polynomial. Moreover, this represents the canonical modular integral for $\psi_{k,m}$ whenever $|m| \leq \ell$.

However, it is possible to consider a much larger class of period functions than simply polynomials. One case frequently studied is the case of rational period functions. This class of functions is discussed in [42], and a complete classification of rational period functions for the full modular group was obtained in [8] (see also [58]). It is also possible to consider period functions which are not rational functions. For example, William Duke has pointed out that $\Delta^{1/6}$ is a weight 2 period function for the full modular group. In these more general cases, computation of the canonical modular integral has proven to be more difficult.

Using weakly holomorphic modular forms, however, it is possible to study the coefficients of canonical modular integrals in a more general framework. For example, one has the following result, based on the same idea appearing in the proof of Proposition 6 and generalized in the arguments used in Chapter 2.

Proposition 51. *(Duke) Let k be an even integer and let ψ be a period function of weight k for the full modular group. Then if we consider the canonical modular integral $F_\psi(\tau) = \sum_{m>\ell} c(m) q^m$, we have the following integral representation of the coefficient $c(m)$:*

$$c(m) = \int_i^\rho \psi(z) f_{2-k,m}(z) dz,$$

where the inetgral is along the circular arc from i to $\rho = e^{\pi i/3}$. Also, if Im(τ) is sufficiently large, we have

$$\frac{F_\psi(\tau)}{f_k(\tau)} = \int_i^\rho \frac{f_{2-k}(z)\psi(z)}{j(z) - j(\tau)} dz, \tag{5.3.3}$$

where j denotes the usual modular invariant.

Proof. As in the proof of Proposition 9 and Theorem 13, the key idea is to consider a truncated fundamental domain. In this case, consider the truncated fundamental domain $\mathfrak{F}(Y)$ for the fundamental domain $\mathfrak{F}$ of $G_3\backslash\mathbb{H}$:

$$\mathfrak{F}(Y) = \{z \in \mathfrak{F} : \text{Im} z \leq Y\}.$$

Integrate $F_\psi(z) f_{2-k}(z)$ around the boundary of $\mathfrak{F}(Y)$, oriented positively. Since this function is holmorphic, the integral equals zero. On the other hand, the integrals along the left and right hand sides cancel, while the integral along the top is $-c(m)$, since $f_{2-k,m}$

$$\begin{aligned} f_{2-k,m}(\tau) &= q^{-m} + O\left(q^{-\ell}\right), \\ F_\psi(\tau) &= O\left(q^{\ell+1}\right), \end{aligned}$$

and $d\tau = \frac{dq}{2\pi i q}$, so the constant term in the q series of the integrand with respect to dq is precisely $-c(m)$.

Meanwhile, on the circular arc comprising the bottom of the boundary, the contribution to the integral equals

$$\int_{-\overline{\rho}}^{i} F_\psi(z) f_{2-k,m}(z)dz + \int_{i}^{\rho} F_\psi(z) f_{2-k,m}(z)dz.$$

Making the change of variables $z = -1/w$ in the first integral, we can rewrite it as

$$\int_\rho^i F_\psi\left(-\frac{1}{w}\right) f_{2-k,m}\left(-\frac{1}{w}\right)\frac{dw}{w^2} = \int_\rho^i w^{-k} F_\psi\left(-\frac{1}{w}\right) f_{2-k,m}(w)dw,$$

using the transformation properties of f_{2-k}. Therefore the contribution from the bottom piece of the boundary equals

$$\int_i^\rho \left(F_\psi(z) - z^{-k}F_\psi\left(-\frac{1}{z}\right)\right) f_{2-k,m}(z)dz = \int_i^\rho \psi(z) f_{2-k,m}(z)dz,$$

since ψ is the period function associated to F_ψ. This completes the first part of the proposition.

To prove the second part, one must make use of the following generating function identity proven in [15]:

$$\frac{f_{2-k}(z)f_k(\tau)}{j(z)-j(\tau)} = \sum_{m>\ell} f_{2-k,m}(z)q^m. \tag{5.3.4}$$

The sum on the right hand side converges uniformly on compact sets in z when $\tau \in \mathbb{H}$ is fixed and $\mathrm{Im} z < \mathrm{Im}\tau$. In particular, this means that for $\mathrm{Im}\tau$ sufficiently large, we have

$$\begin{aligned} \int_i^\rho \frac{f_k(\tau)f_{2-k}(z)\psi(z)}{j(z)-j(\tau)}dz &= \sum_{m>\ell}\left(\int_i^\rho \psi(z)f_{2-k,m}(z)dz\right)q^m \\ &= F_\psi(\tau), \end{aligned}$$

as claimed. □

5.3.2. A connection to Atkin polynomials. What does any of this have to do with Atkin polynomials? To answer this question, suppose we have a period function that satisfies the following additional symmetry condition:

$$\overline{\psi(z)} = \psi\left(-\overline{z}\right).$$

Consider the function

$$u(z) = iz\psi\left(z\right) f_{2-k}\left(z\right).$$

On the unit circle $\overline{z} = \frac{1}{z}$, by the transformation properties of ψ and f_{2-k} we obtain

$$\begin{aligned}\overline{u(z)} &= -i\overline{z}\overline{\psi\left(z\right)f_{2-k}\left(z\right)} \\ &= -\frac{i}{z}\psi\left(-\frac{1}{z}\right)f_{2-k}\left(-\frac{1}{z}\right) \\ &= -\frac{i}{z}\left[-z^k\psi\left(z\right)\right]\left[z^{2-k}f_{2-k}\left(z\right)\right] \\ &= u(z),\end{aligned}$$

so that u is real-valued.

We can relate u to F_ψ by means of the second part of Proposition 51, which is now equivalent to the statement that

$$\frac{F_\psi(\tau)}{f_k(\tau)} = \int_\rho^i \frac{u(z)}{j(\tau) - j(z)}\frac{dz}{iz}.$$

Now suppose we change variables from z to J via the equality $z = \frac{\Phi_3(J(z))}{2\pi i}$ where $J(z) = J_3(z)$ is the normalization of the j invariant as in the previous chapters. Then we can rewrite the above integral as

$$1728\frac{F_\psi(\tau)}{f_k(\tau)} = \int_0^1 \frac{w_\psi(J)}{J(\tau) - J}dJ,$$

where

$$w_\psi(J) = \frac{u(J)\Phi_3'(J)}{i\Phi_3(J)},$$

and we have committed a slight abuse of notation by writing $u(J)$ for $u(z(J))$. The similarity between this expression and the expresion for the generalized Atkin weight $w_{m,k}$ given by (2.2.8) in the case $m = 3, k = 1$ is not a coincidence. Indeed, if we consider the weight two period function $\psi(z) = \frac{6i}{\pi z}$ (the proof that this is indeed a weight 2 period function is given in the next section), then $u(z) = \frac{6}{\pi}$ since $f_0 = 1$, and the weight $w_\psi(J)$ reduces to

$$w_\psi(J) = \frac{6}{\pi i}\frac{\Phi_3'(J)}{\Phi_3(J)} = w_3(J).$$

In other words, the weight associated to ψ is the Atkin weight.

In this case, the left hand side of 5.3.3 reduces to $1728\frac{E_2\Delta}{E_4E_6^2}$, and the right hand side reduces to

$$\frac{1}{J(\tau)}\sum_{k=0}^{\infty}\frac{1}{J(\tau)^k}\int_0^1 J^k w_\psi(J)dJ$$

for Imτ sufficiently large. In other words, we have recovered the fact that this power series generated by the moments of the Atkin weight is equal to the negative of $\frac{d \log \Delta}{dJ}$, which is precisely the statement proven by Kaneko and Zagier and generalized in Chapter 2.

5.3.3. Generalizations to Atkin-type polynomials. It is possible to extend this theory of period functions to a larger class of groups. In particular, if one replaces the functional equation (5.3.2) by the equation

$$\psi \mid_k \left(\sum_{\ell=0}^{m-1} U_m^\ell \right) = 0, \tag{5.3.5}$$

where where $U_m = ST_m = \pm \begin{pmatrix} 0 & -1 \\ 1 & \lambda_m \end{pmatrix}$ and $\lambda_m = 2\cos(\pi/m)$, then we say that ψ is a period function for the Hecke triangle group G_m. The slash operator has the same meaning here as in the case of the full modular group. We can also define a modular integral in an analogous way; the only change is in the description of the Fourier expansion, where we require

$$F(\tau) = \sum_n a(n) q_m^n,$$

with $q_m = e^{2\pi i \tau/\lambda_m}$. The other conditions remain the same. Period functions for the Hecke groups have been studied in [12], and the specific case of period functions for Hecke triangle groups which are polynomials in $\log(\tau)$ is discussed in [25]. Similar polynomials for non-discrete groups are discussed in [26].

As we have just seen, from the perspective of period functions, the Atkin weight is the weight associated to a constant multiple of the period function $\psi(\tau) = \frac{1}{\tau}$. However, according to the following lemma, this function is not just a period function for G_3.

Lemma 52. *For any integer $m \geq 3$, the function $\psi(\tau) = \frac{1}{\tau}$ is a period function for G_m of weight 2.*

This follows from a stronger classification result on rational period functions for Hecke triangle groups (see [12]). It is also possible to prove the statement directly using only basic linear algebra and trigonometry.

The fact that $\psi(\tau) = \frac{1}{\tau}$ is a period function for each triangle group G_m suggests that it should be possible to develop an analogous theory of Atkin polynomials for each of these groups. Indeed, it's possible to begin with the theory of period functions, and use this as motivation to study polynomials which are orthogonal with respect to the weight function w_ψ, provided the mapping $\psi \mapsto w_\psi$ does actually give rise to a weight function from the viewpoint of the theory of orthogonal polynomials.

From this perspective, we see by (2.1.11) that for fixed $m \geq 3$ the function

$$\psi(\tau) = \frac{\lambda_m}{2\pi i \alpha_m \tau}$$

is a period function of weight 2 for G_m with corresponding modular integral $E_{2,m}$. We would like to develop a general formula for the Fourier coefficients of modular integrals as in Proposition 51 above, but to do this we first need an analogue of the weakly holomorphic modular forms discussed in the previous section.

Before we construct such forms, we provide a bit more background on the spaces of modular forms for the Hecke triangle groups. For fixed m, a modular form for G_m of weight k and multiplier $\nu = \pm 1$ is a holomorphic function f on the upper half plane that satisfies the transformation laws

$$\begin{aligned} f\left(T_m \tau\right) &= f(\tau), \\ f\left(S\tau\right) &= \nu \left(-\frac{1}{i\tau}\right)^{-k} f(\tau), \end{aligned}$$

is holomorphic at infinity, and whose Fourier coefficients satisfy the growth condition

$$a(n) \ll n^c$$

for some constant c, where

$$f(\tau) = \sum_{n=0}^{\infty} a(n) q_m^n.$$

When k and ν are fixed, the space of such forms will be denoted by $\mathcal{M}_{k,\nu,m}$.

$\mathcal{M}_{k,\nu,m}$ is always empty unless

$$k = \frac{r}{m\alpha_m} + 1 - \nu \tag{5.3.6}$$

for some positive integer r, in which case it has dimension

$$1 + \left\lfloor \frac{r + (\nu - 1)/2}{m} \right\rfloor = 1 + \left\lfloor k\alpha_m + \frac{\nu - 1}{4} \right\rfloor.$$

For example, when $m = 3$, $\nu = -1$ when k is congruent to 2 mod 4, and $\nu = 1$ when k is congruent to 0 mod 4. In this case the dependence on the multiplier is usually ignored because the transformation rules simplify. In particular, we see that for any even $k > 2$, exactly one of $\mathcal{M}_{k,1,3}$ and $\mathcal{M}_{k,-1,3}$ is empty, but this need no longer be true for general m. For more on spaces of modular forms for Hecke triangle groups, see [36] and the references therein.

As in the case of the full modular group, we define the space of weakly holomorphic modular forms of weight k and multiplier $\nu = \pm 1$ for the Hecke group G_m to be the space of holomorphic functions f on the upper half plane satisfying the same transformation properties as in the holomorphic case, but we allow for negative n values in the Fourier expansion - i.e. we allow for poles at the cusp. Denote this space by $\mathcal{M}^!_{k,\nu,m}$.

Fix a value m and a weight k such that $\mathcal{M}^!_{k,\nu,m}$ is nonempty. Let $\ell \in \mathbb{Z}$ and $0 \leq r < m$ be the unique integers such that

$$k = \frac{\ell}{\alpha_m} + \frac{r}{m\alpha_m} + \frac{1-\nu}{4\alpha_m}; \tag{5.3.7}$$

such integers exist because of the restriction (5.3.6). Keeping the notation from Chapter 2, let f_0 and f_i be the unique modular forms in $\mathcal{M}_{\frac{4}{m-2},1,m}$ and $\mathcal{M}_{\frac{2m}{m-2},-1,m}$, and let Δ_m be the unique cusp form of weight $1/\alpha_m$ and multiplier 1 (note this is the smallest value of k for which the space of modular forms has dimension greater than 1).

For each $m_1 \geq -\ell$, there exists a unique $f_{k,m_1,m} \in \mathcal{M}^!_{k,\nu,m}$ such that

$$f_{k,m_1,m}(\tau) = q_m^{-m_1} + O\left(q_m^{\ell+1}\right).$$

This form can be constructed quite explicitly, as in the case $m = 3$: we simply take

$$\begin{aligned} f_{k,m_1,m} &= \Delta_m^\ell f_0^r f_i^{\frac{1-\nu}{2}} P_{k,m_1,m}\left(j_m\right) \\ &= q_m^{-m_1} + \sum_{n>\ell} a_k\left(m_1,n\right) q_m^n. \end{aligned}$$

where P is a monic polynomial of degree $m_1 + \ell$, and is determined by the restriction that the Fourier coefficients $a_k(m_1,n)$ of $f_{k,m_1,m}$ are equal to zero for $-m_1 < n < \ell + 1$. Also, $j_m = J_m/A_m$. Note that unlike the case $m = 3$, the coefficients $a_k\left(m_1,n\right)$ need not be integers, though we do know that $a_k\left(m_1,n\right) A_m^n$ is rational, since it is shown in [77] that the Fourier coefficients of modular forms for the group G_m can always be written in the form

$$a(n) = \tilde{a}(n) A_m^{-n},$$

where $\tilde{a}(n) = a(n)A_m^n$ is rational. As before, in the case $m_1 = -\ell$ we write $f_k = f_{k,-\ell,m}$. Of course, this function depends on m, but since m is fixed this should cause no confusion.

For example, if we denote the Fourier expansion of J_m by

$$J_m(\tau) = \frac{A_m}{q_m} + \sum_{n\geq 0} a_m(n) A_m^{-n} q_m^n$$

for some rational coefficients $a_m(n)$, then when $k = 0$ we have

$$\begin{aligned} P_{0,0,m} &= 1, \\ P_{0,1,m} &= \frac{J_m}{A_m} - \frac{a_m(0)}{A_m} \\ &= j_m - \frac{a_m(0)}{A_m}, \\ P_{0,2,m} &= j_m^2 - 2\frac{a_m(0)}{A_m} j_m + \frac{a_m(0)^2}{A_m^2} - 2\frac{a_m(1)}{A_m^2}. \end{aligned}$$

In general, we see that $A_m^{m_1} P_{0,m_1,m}(j_m)$ is a polynomial of degree m_1 in J_m with rational coefficients.

These weakly holomorphic modular forms for G_m turn out to satisfy the same type of generating function identity as (5.3.4); indeed, the proof is nearly identical to the one provided in [15]. For sake of completeness we provide a brief proof here.

Proposition 53. *Fix an $m \geq 3$. For any k of the form (5.3.7) we have*

$$\sum_{m_1 \geq -\ell} f_{k,m_1,m}(z) q_m^{m_1} = \frac{f_k(z) f_{2-k}(\tau)}{j_m(\tau) - j_m(z)}.$$

Proof. By definition of the form $f_{k,m_1,m}$, we have

$$\Delta_m^\ell f_0^r f_i^{\frac{1-\nu}{2}} P_{k,m_1,m}\left(j_m\right) = q_m^{-m_1} + O\left(q^{\ell+1}\right) \tag{5.3.8}$$

Let C' denote a circular contour oriented centered at 0 in the positive direction. When the radius is sufficiently large, since P is a polynomial, we have

$$\begin{aligned} P_{k,m_1,m}\left(\zeta\right) &= \frac{1}{2\pi i} \int_{C'} \frac{P_{k,m_1,m}\left(j_m\right)}{j_m - \zeta} dj_m \\ &= \frac{1}{2\pi i} \int_{C'} \frac{q_m^{-m_1}}{\Delta_m^\ell f_0^r f_i^{\frac{1-\nu}{2}} \left(j_m - \zeta\right)} dj_m, \end{aligned}$$

by (5.3.8).

We see from Lemma 8 and (2.1.10) that

$$\frac{dj_m}{dq_m} = -\frac{f_0^{m-1} f_i}{q\Delta_m}, \tag{5.3.9}$$

so by changing variables from j_m to q_m we can write the above integral as

$$\frac{1}{2\pi i} \int_C \frac{f_0(\tau)^{m-1-r} f_i(\tau)^{\frac{v+1}{2}} \Delta_m(\tau)^{-\ell-1}}{j_m(\tau) - \zeta} q_m^{-m_1-1} dq_m$$

for some circular contour C centered at 0 of sufficiently small radius (notice that the negative sign in (5.3.9) ensures that the curve C still has a positive orientation). By choice of k, along with the fact that

$$\frac{1}{2\alpha_m} - \frac{1}{m\alpha_m} = 2$$

for any m, the numerator in the integral is simply $f_{2-k}(\tau)$. Therefore, if we replace ζ by $j_m(z)$ and multiply both sides by $f_k(z)$, we have

$$\begin{aligned} f_{k,m_1,m}(z) &= f_k(z)P_{k,m_1,m}(z) \\ &= \frac{1}{2\pi i}\int_C \frac{f_k(z)f_{2-k}(\tau)}{j_m(\tau)-j_m(z)} q_m^{-m_1-1}dq_m. \end{aligned}$$

The result now follows from an application of Cauchy's integral formula. □

As in the case of $m = 3$, the above proposition implies the following duality result:

Corollary 54. *Fix an $m \geq 3$. For any k of the form (5.3.7) we have the equality*

$$a_k(m_1, n) = -a_{2-k}(n, m_1)$$

between the Fourier coefficients of the modular forms $f_{k,m_1,m}$ and $f_{2-k,n,m}$.

We can also use the above proposition to generalize Proposition 51 from the previous section. The proof is nearly identical, so we merely supply the statement.

Proposition 55. *Fix an $m \geq 3$. For any k of the form (5.3.7) let ψ be a period function of weight k for the Hecke triangle group G_m. Then given a modular integral $F_\psi(\tau) = \sum_{m_1 > \ell} c(m_1)q_m^{m_1}$, we have the following integral representation of the coefficient $c(m_1)$:*

$$c(m_1) = \frac{1}{\lambda_m}\int_i^{\rho_m} \psi(z)f_{2-k,m_1}(z)dz,$$

where the integral is along the circular arc from i to $\rho = e^{\pi i/m}$. Also, if Im(τ) is sufficiently large, we have

$$\frac{F_\psi(\tau)}{f_k(\tau)} = \frac{1}{\lambda_m}\int_i^{\rho_m} \frac{f_{2-k}(z)\psi(z)}{j_m(z)-j_m(\tau)}dz. \tag{5.3.10}$$

In particular, if we take $\psi(\tau) = \frac{\lambda_m}{2\pi i\alpha_m\tau}$ so that $F_\psi = E_{2,m}$, then keeping with the notation of the previous section we have $u(J) = \lambda_m/2\pi\alpha_m$, so that (5.3.10) becomes

$$A_m^{-1}\frac{F_\psi(\tau)}{f_k(\tau)} = \int_0^1 \frac{w_m(J)}{J(\tau)-J}dJ.$$

In other words, we still have $w_\psi = w_m$, so the period function gives rise to a generalized Atkin weight, and the second statement of the above proposition is equivalent to Proposition 10.

5.3.4. Coefficients of certain modular integrals. Our last topic in this section concerns a different family of period functions for the Hecke triangle groups G_m. As mentioned earlier in this chapter, when $m = 3$ the canonical cusp form Δ gives rise to a period function proportional to $\Delta^{1/6}$ of weight 2 for the full modular group. In fact, this observation can be generalized as follows.

Theorem 56. *Fix an $m \geq 3$. Then the function*

$$-\frac{2\pi}{A_m^{2\alpha_m}}\Delta_m^{2\alpha_m}(\tau) = -\frac{2\pi}{J_m(\tau)^{2\alpha_m}}\,{}_2F_1\left(\alpha_m, \beta_m; 1; \frac{1}{J_m(\tau)}\right)^2$$

is a period function of weight 2 for the full modular group G_m, where Δ_m is the canonical cusp form on this group as defined in Chapter 2. Moreover, the weight associated to this period function is a Jacobi weight of the form (5.1.1), rescaled to $[0,1]$, with $\alpha = 1/2$ and $\beta = 1/2 - 2\alpha_m$.

Proof. To show that the above function is a period function, it suffices to show that $\Delta_m^{2\alpha_m}$ is a period function. Since Δ_m is a cusp form, the growth conditions necessary in the definition of a period function are met (for more on the growth of cusp forms near the boundary in the case $m = 3$, see [38]). The transformation rule (5.3.1) follows from analytic continuation of the functional equation for the hypergeometric function given in Proposition 14. In particular, we see that

$$\Delta_m^{2\alpha_m}\left(-\frac{1}{\tau}\right) = -\tau^2\Delta_m(\tau).$$

On the other hand, we know that for $|q_m|$ sufficiently small, since Δ_m is λ_m periodic, holomorphic on the upper half plane, and has vanishing 0^{th} Fourier coefficient, it has a product expansion

$$\Delta_m(\tau) = q_m \prod_{n\geq 1}(1 - q_m^n)^{c(n)}$$

for some explicitly computable constants $c(n)$ (see [6, 17]). From this, since the cusp form is nonvanishing on the upper half plane, it follows that

$$\Delta_m^{2\alpha_m}(\tau + \lambda_m) = e^{4\pi i\alpha_m}\Delta_m^{2\alpha_m}(\tau).$$

Combining these two transformation rules, we deduce that

$$\Delta_m^{2\alpha_m}(U_m\tau) = -e^{4\pi i\alpha_m}(z + \lambda_m)^2\,\Delta_m^{2\alpha_m}(\tau),$$

and more generally

$$\Delta_m^{2\alpha_m}\left(U_m^\ell\tau\right) = -e^{4\pi i\alpha_m}\left(c_\ell z + d_\ell\right)^2 \Delta_m^{2\alpha_m}\left(\tau\right),$$

where

$$U_m^\ell = \left(\begin{array}{cc} * & * \\ c_\ell & d_\ell \end{array}\right).$$

In particular, this means

$$\Delta_m^{2\alpha_m}\mid_2 U^\ell(\tau) = \left(-e^{4\pi i\alpha_m}\right)^\ell \Delta_m^{2\alpha_m}(\tau),$$

so that

$$\begin{aligned} \Delta_m^{2\alpha_m}\Bigg|_2 \left(\sum_{\ell=0}^{m-1} U_m^\ell\right)(\tau) &= \Delta_m^{2\alpha_m}(\tau)\sum_{\ell=0}^{m-1} -e^{4\pi i\alpha_m \ell} \\ &= \Delta_m^{2\alpha_m}(\tau)\sum_{\ell=0}^{m-1} e^{-2\pi i\ell/m} \\ &= 0. \end{aligned}$$

Therefore $\Delta_m^{2\alpha_m}$ is indeed a period function.

To find the weight associated to the rescaled version of this function given in the statement of the theorem, we recall that the Atkin weight for fixed m can be written as

$$\begin{aligned} w_m(J) &= \frac{1}{2\pi i\alpha_m}\frac{\Phi'_m(J)}{\Phi_m(J)} \\ & \frac{-A_m^{2\alpha_m}}{2\pi\alpha_m J^{1/2+2\alpha_m}(1-J)^{1/2}\Delta_m\left(\frac{\lambda_m}{2\pi i}\Phi_m(J)\right)^{2\alpha_m}\Phi_m(J)} \end{aligned}$$

by Corollary 12. Using this, we see that if we fix our period function as

$$\psi(\tau) = -\frac{2\pi}{A_m^{2\alpha_m}}\Delta_m^{2\alpha_m}(\tau),$$

the fact that $k = 2$ implies

$$u_\psi(z) = -iz\frac{2\pi}{A_m^{2\alpha_m}}\Delta_m^{2\alpha_m}(z),$$

and so

$$\begin{aligned} w_\psi(J) &= \frac{u_\psi(J)\Phi'_m(J)}{\lambda_m i\Phi_m(J)} \\ &= \frac{2\pi\alpha_m}{\lambda_m} u_\psi(J) w_m(J) \\ &= \frac{2\pi iz}{\lambda_m J^{1/2+2\alpha_m}(1-J)^{1/2}\Phi_m(J)} \\ &= \frac{1}{J^{1/2+2\alpha_m}(1-J)^{1/2}}, \end{aligned}$$

since $2\pi iz/\lambda_m = \Phi_m(J)$. Therefore the weight is indeed a Jacobi weight, as claimed. □

We can use the above result, along with Proposition 55, to investigate the coefficients of the modular integral associated to $-\frac{2\pi}{A_m^{2\alpha_m}}\Delta_m^{2\alpha_m}$. We obtain the following result:

PROPOSITION 57. *Let $\psi(\tau) = -\frac{2\pi}{A_m^{2\alpha_m}}\Delta_m^{2\alpha_m}(\tau)$ be the weight 2 period function from above. Also, for each $m_1 \geq 0$, let $b_{m_1}(\ell)$ denote the (rational) coefficient of J_m^ℓ in $A_m^{m_1}P_{0,m_1,m}(j_m)$, i.e.*

$$A_m^{m_1}P_{0,m_1,m}(j_m) = \sum_{\ell=0}^{m_1} b_{m_1}(\ell) J_m^\ell.$$

Then the modular integral $F_\psi(\tau) = \sum_{m_1\geq 0} c(m_1)q_m^{m_1}$ satisfies

$$c(m_1) = \frac{-\sqrt{\pi}}{A_m^{m_1}}\frac{\Gamma\left(\frac{1}{2}-2\alpha_m\right)}{\Gamma(1-2\alpha_m)}\sum_{\ell=0}^{m_1} b_{m_1}(\ell)\frac{\left(\frac{1}{2}-2\alpha_m\right)_\ell}{(1-2\alpha_m)_\ell}$$

PROOF. First, note that when $k=2$, we have

$$\ell + \frac{r}{m} + \frac{1-\nu}{4} = 2\alpha_m = \frac{m-2}{2m}$$

for some $\ell \in \mathbb{Z}$, $0 \leq r < m$, and $\nu \in \{\pm 1\}$. This is equivalent to the statement

$$m\left(2\ell + \frac{1-\nu}{2} - 1\right) = -2 - 2r,$$

and since the right hand side is nonzero, both sides must be divisible by m, i.e. $r = m-1$. In turn, this forces $\nu = -1$ and $\ell = -1$, so the Fourier series for F_ψ begins with the constant term, as claimed.

To find the formula for the Fourier coefficients, we apply the integral representation of the coefficients given in Proposition 55. Indeed, since

$$\Phi'_m(J) = \frac{A_m^{2\alpha_m}}{iJ^{1/2+2\alpha_m}(1-J)^{1/2}\Delta_m^{2\alpha_m}}$$

we have

$$\begin{aligned} c\left(m_1\right) &= \frac{1}{\lambda_m}\int_i^{\rho_m}\psi(z)f_{0,m_1}(z)dz \\ &= \frac{1}{2\pi i}\int_1^0\psi(J)P_{0,m_1,m}\left(J\right)\Phi_m'(J)dJ \\ &= -\int_0^1\frac{P_{0,m_1,m}(J)}{J^{1/2+2\alpha_m}\left(1-J\right)^{1/2}}dJ. \end{aligned}$$

Using the given information on the coefficients of $P_{0,m_1,m}(J)$, we can rewrite the above integral as

$$\begin{aligned} & -\frac{1}{A_m^{m_1}}\int_0^1\sum_{\ell=0}^{m_1}b_{m_1}\left(\ell\right)J_m^{\ell-1/2-2\alpha_m}(1-J)^{-1/2}dJ \\ = & -\frac{1}{A_m^{m_1}}\sum_{\ell=0}^{m_1}b_{m_1}\left(\ell\right)\frac{\Gamma\left(\frac{1}{2}-2\alpha_m+\ell\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(1-2\alpha_m+\ell\right)} \\ = & \frac{-\sqrt{\pi}}{A_m^{m_1}}\frac{\Gamma\left(\frac{1}{2}-2\alpha_m\right)}{\Gamma\left(1-2\alpha_m\right)}\sum_{\ell=0}^{m_1}b_{m_1}\left(\ell\right)\frac{\left(\frac{1}{2}-2\alpha_m\right)_\ell}{\left(1-2\alpha_m\right)_\ell}, \end{aligned}$$

as claimed. □

In particular, for this period function, the modular integral has a transcendental factor which can easily be factored out. The transcendental factor only depends on m_1 through the value of A_m, so in particular, when $m \in \{3, 4, 6, \infty\}$ we obtain the following corollary:

Corollary 58. *Let $m \in \{3, 4, 6, \infty\}$, and keep the notation as in the previous proposition. Then the Fourier coefficients $c\left(m_1\right)$ of the modular integral associated to any scalar multiple of $\Delta_m^{2\alpha_m}$ satisfy*

$$\frac{c\left(m_1\right)}{c(0)} \in \mathbb{Q}.$$

In other words, up to renormalization, the coefficients of the Fourier expansion of the modular integral are rational. In the case $m = 3$, this shows that the Fourier coefficients of a suitable multiple of the modular integral $F_{\Delta^{1/6}}$ are rational, a fact which appears to be new.

Bibliography

[1] G. E. Andrews, R. Aske, R. Roy. *Special Functions.* Cambridge University Press, Cambridge, UK, 1999.

[2] N. Archinard. "Hypergeometric abelian varieties." *Canad. J. Math.,* **55**(5):897-932, 2003.

[3] Archinard, N. "Exceptional sets of hypergeometric series." *J. Number Theory,* 101:244–269, 2003.

[4] O. Billet and M. Joye. "The Jacobi model of an elliptic curve and side-channel analysis." *Applied Algebra, Algorithms and Error-Correcting Codes, LNCS*, **2643**:34-42, 2003.

[5] J. Brillhart, P. Morton. "Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial." *J. Number Theory,* **106**:79-111, 2004.

[6] J. H. Bruinier, W. Kohnen, and K. Ono. "Values of modular functions and the divisors of modular forms." *Compositio Math.,* **140**:552-566, 2004.

[7] C. Caratheodory. *Theory of functions of a complex variable II.* Chelsea, New York, second edition, 1960.

[8] Y. Choie and D. Zagier. "Rational period functions for PSL(2,Z)." In *A tribute to Emil Grosswald: Number theory and related analysis* (eds. M. Knopp and M. Sheingorn). Vol. 143 of *Contemporary Mathematics Series*, pp. 89-108. American Mathematical Society, Providence, RI, 1993.

[9] D.V. Chudnovsky and G.V. Chudnovsky. "Transcendental Methods and Theta-Functions." *Proc. Syp. Pure Mathematics* **49**(2):167-232. American Mathematical Society, Providence, RI, 1989.

[10] P. Cohen, J. Wolfart. "Modular embeddings for some non-arithmetic Fuchsian groups." *Acta Arith.,* **56**:93-110, 1990.

[11] P. Cohen, G. Wüstholz. "Application of the André-Oort conjecture to some questions in transcendence." In *A Panorama of Number Theory or the View from Baker's Garden* (ed. G. Wüstholz), pp. 89-106. Cambridge University Press, Cambridge, UK, 2002.

[12] W. Culp-Ressler. "Rational period functions on the Hecke groups." *Ramanujan J.* **5**:281-294, 2001.

[13] F. Diamond, J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[14] P. A. Deift. *Orthgonal polynomials and random matrices: a Riemann-Hilbert approach,* volume 3 of *Courant Lecture Notes in Mathematics.* New York University, Courant Institute of Mathematical Sciences, New York; American Mathematical Society, Providence, RI, 1999.

[15] W. Duke and P. Jenkins. "On the zeros and coefficients of certain weakly holomorphic modular forms." *Pure Appl. Math. Q.,* **4**(4, part 1):1327-1340, 2008.

[16] C.J. Earle. "Some Jacobian varieties which split." In *Lecture Notes in Mathematics*, vol. 747, pp. 101-107. Springer-Verlag, Berlin, Heidelberg, New York, 1979.

[17] W. Eholzer and N.-P. Skoruppa. "Product expansions of conformal characters." *Phys. Lett. B,* **388**:82-89, 1996.

[18] T. Ekedahl. "On supersingular curves and Abelian varieties." *Math. Scand.,* **60**:151-178, 1987.

[19] V. Enolski and P. Richter. "Periods of hyperelliptic integrals expressed in terms of $\theta-$constants by means of Thomae formulae." *Phil. Trans. R. Soc. A,* **366**:1005-1024, 2008.

[20] L. R. A. Finotti. "A formula for the supersingular polynomial." *Acta Arith.,* **139**(3):265-273, 2009.

[21] S. D. Galbraith. "Supersingular curves in cryptography." In *ASIACRYPT 2001* (ed. C. Boyd), pp. 495-513. Springer LNCS **2248**, 2001.

[22] J. González. "Hasse-Witt matrices for the Fermat curves of prime degree." *Tohoku Math. J.,* **49**(2):149-163, 1997.

[23] R. E. Green, S. G. Krantz. *Function theory of one complex variable.* Graduate Studies in Mathematics, Volume 40. American Mathematical Society, Providende, RI, third edition, 2006.

[24] A. Guillevic, D. Vergnaud. "Genus 2 hyperelliptic curve families with explicity Jacobian order evaluation and pairing-friendly constructions." *Cryptology ePrint Archive*, Report 2011/604, http://eprint.iacr.org/, 2011.

[25] A. Hassen. "Log-polynomial period functions for Hecke groups." *Ramanujan J.*, **3**(2):119-151, 1999.

[26] A. Hassen. "Log-polynomial period functions for nondiscrete Hecke groups." *Proc. Amer. Math. Soc.,* **128**:387-396, 2000.

[27] E. Hecke. "Uber die Bestimmung Dirichletscher Reihin durch ihre Funktionalgleichung." *Math. Ann.,* **112**:664-699, 1936.

[28] E. Hecke. *Dirichlet Series, Modular Functions and Quadratic Forms.* Edwards Brothers, Inc., Ann Arbor, 1938.

[29] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2004.

[30] J. I. Hutchinson. "On a class of automorphic functions." *Trans. Amer. Math. Soc.*, **3**(1):1–11, 1902.

[31] T. Ibukiyama, T. Katsura, F. Oort. "Supersingular curves of genus two and class numbers." *Compositio Math.*, **57**(2):127-152, 1986.

[32] J. Igusa. "On the transformation theory of elliptic functions." *Amer. J. Math.,* **81**:436-452, 1959.

[33] Y. Ihara. "Schwarzian equations." *J. Fac. Sci. Univ. Tokyo Sect. IA Math.,* **21**:97-118, 1974.

[34] K. Ireland, M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[35] M. E. H. Ismail. *Classical and quantum orthogonal polynomials in one variable*. Cambridge University Press, Cambridge, UK, 2005.

[36] J. Kaczorowski, G. Molteni, A Perelli, J. Steuding, J. Wolfart. "Hecke's theory and the Selberg class." *Funct. Approx. Comment. Math.,* **35**:183-194, 2006.

[37] B. Kane. "Faber polynomials and Poincaré series." *Math. Res. Lett.*, **18**(4):591-611, 2011.

[38] B. Kane, K. Bringmann, W. Kohnen. "On the boundary behavior of automorphic forms." *Int. J. of Number Theory*, **2**(2):187-194, 2006.

[39] S. Katok. *Fuchsian groups*. Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1992.

[40] M. Kaneko, D. Zagier. "Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials." In *Computational Perspectives on Number Theory* (Chicago, IL, 1995), *AMS/IP Stud. Adv. Math.*, **7**:97-126, American Mathematical Society, Providence, RI, 1998.

[41] M. I. Knopp. "Some new results on the Eichler cohomology of automorphic forms." *Bull. Amer. Math. Soc.,* **80**:607-632, 1974.

[42] M. I. Knopp. "Rational period functions of the modular group." With an appendix by Georges Grinstein. *Duke Math. J.*, **45**(1):47-62, 1978.

[43] S. Koizumi. "Remarks on Takase's paper 'a generalization of Rosenhain's normal form with application'." *Proc. Jpn Acad.*, **73**:12-13, 1997.

[44] R. Küstner. "Mapping properties of hypergeometric functions and convolutions of starlike or convex functions of order α." *Comput. Methods Funct. Theory*, **2**:597-610, 2002.

[45] P. Landweber. "Supersingular elliptic curves and congruences for Legendre polynomials." In *Elliptic Curves and Modular Forms in Algebraic Topology*, (ed. Landweber), pp. 69-93. Springer Lecture Notes, **1326**, Springer, Berlin, 1988.

[46] J. Lehner. "Note on the Schwarz triangle functions." *Pacific J. Math.*, **4**:243-249, 1954.

[47] J. Leo. "Fourier coecients of triangle functions." PhD thesis, UCLA, 2008.

[48] F. Leprévost, F. Morain. "Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractéres." *J. Number Theory*, **64**:165-182, 1997.

[49] R. Lercier and C. Ritzenthaler. "Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects." Eprint arXiv:1111.4152, 2011.

[50] R. Lercier, C. Ritzenthaler, J. Sijsling. "Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent." To appear in the *Proceedings of the Tenth Algorithmic Number Theory Symposium* (ANTS-X), Mathematical Sciences Publishers, July 2012.

[51] E. Lucas. "Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier." *Bulletin de le Société Mathématique de France*, **6**:49-54, 1878.

[52] Yu. I. Manin. "The theory of commutative formal groups over fields of finite characteristic." *Russian Math. Surveys,* **18**:1-83, 1963.

[53] R. Morris. "On the automorphic functions of the group (0,3; l_1, l_2, l_3)." *Trans. Amer. Math. Soc.*, **7**:425-448, 1906.

[54] Z. Nehari. *Conformal mapping.* McGraw-Hill Book Co., Inc., New York, Toronto, London, 1952.

[55] N. Nygaard. "Slopes of powers of Frobenius on crystalline cohomology." *Ann. Sci. École Norm. Sup.*, **14**(4):369-401, 1981.

[56] N. Nygaard. "On supersingular abelian varieties." *Algebraic geometry* (Ann Arbor, Mich., 1981), 83-101, *Lecture Notes in Math.*, **1008**, Springer, Berlin-New York, 1983.

[57] F. Oort. "Subvarieties of moduli spaces." *Inv. Math.*, **24**:95–119, 1970.

[58] L.A. Parson. "Rational period functions and indefinite binary quadratic forms, III." In *A tribute to Emil Grosswald: Number theory and related analysis*, (eds. M. Knopp and M. Sheingorn). Vol. 143 of *Contemporary Mathematics Series*, pp. 109-116. American Mathematical Society, Providence, RI, 1993.

[59] B. Poonen. "Computational aspects of curves of genus at least 2." In *Algorithmic Number Theory II* (ed. H. Cohen), Springer LNCS **1122**:283-306, 1996.

[60] J. Raleigh. "On the Fourier coefficients of triangle functions." *Acta Arith.*, **8**:107-111, 1963.

[61] R. A. Rankin. "The zeros of Eisenstein series, Publications of the Ramanujan Institute." **1**:137-144, 1969.

[62] E.S. Rowland. "The number of nonzero binomial coefficients modulo p^α." arXiv: 1001.1783v2, 2010.

[63] T. Satoh. "Generating genus two hyperelliptic curves over large characteristic finite fields." In *Advances in Cryptology - Eurocrypt 2009* (ed. A. Joux), Springer LNCS **5479**, 2009.

[64] T.A. Schmidt. "Klein's cubic surface and a "non-arithmetic" curve." *Math. Ann.*, **309**(4):533-539, 1997.

[65] H. Shiga and J. Wolfart. "Algebraic values of Schwarz triangle functions." In *Arithmetic and Geometry Around Hypergeometric Functions* (eds. R.-P. Holzapfel, A. M. Uludag and M. Yoshida. Birkhäuser). Progress in Mathematics, **260**:287-312, 2007.

[66] G. Shimura. "On analytic families of polarized abelian varieties and automorphic functions." *Ann. Math.*, **78**:149-192, 1967.

[67] G. Shimura. “Automorphic forms and the periods of abelian varieties.” *J. Math Soc. Japan*, **31**:561-592, 1979.

[68] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[69] G. Szegö. *Orthogonal polynomials.* American Mathematical Society, Colloquium Publications, Vol. 23. American Mathematical Society, Providence, RI, fourth edition, 1975.

[70] K. Takase. “A generalization of Rosenhain’s normal form for hyperelliptic curves with application.” *Proc. Jpn. Acad.,* **72**:162-165, 1996.

[71] K. Takeuchi. “A characterization of arithmetic Fuchsian groups.” *J. Math. Soc. Japan*, **27**:600-612, 1975.

[72] K. Takeuchi. “Arithmetic triangle groups.” *J. Math. Soc. Japan,* **29**:91-106, 1977.

[73] K. Takeuchi. “Commensurability classes of arithmetic triangle groups.” *J. Fac. Sci. Univ. Tokyo, Sec IA*, **24**:201-212, 1977.

[74] J. Thomae. “Beitrag zur Bestimmung von $\vartheta\,(0,0,\ldots,0)$ durch die Klassenmoduln algebraischer Functionen.” *J Reine Angew. Math.* **71**:201-222, 1870.

[75] H. Tsutsumi. “The Atkin orthogonal polynomials for congruence subgroups of low levels.” *Ramanujan J.*, **14**:223–247, 2007.

[76] R. Valentini. “Hyperelliptic curves with zero Hasse-Witt matrix.” *Man. Mathematica*, **86**:185–194, 1995.

[77] J. Wolfart. “Transzendente Zahlen als Fourierkoeffizienten von Heckes Modulformen.” *Acta Arith.*, **39**(2):193-205, 1981.

[78] J. W. Young. “On the group of sign $(0,3;2,4,\infty)$ and the functions belonging to it.” *Trans. Amer. Math. Soc.*, **5**(1):81–104, 1904.

[79] N. Yui. “Jacobi quartics, Legendre polynomials and formal groups.” In *Elliptic Curves and Modular Forms in Algebraic Topology*, (ed. Landweber), pp. 182-215. Springer Lecture Notes, **1326**, Springer, Berlin, 1988.

[80] N. Yui. “On the jacobian varieties of hyper curves over fields of characteristic $p > 0$.” *J. Algebra* **52**:378-410, 1978.

[81] H. Żołądek. *The Monodromy Group.* Birkhäuser, Basel, Switzerland, 2006.