An Algorithm for Numerically Computing Preimages of the j-invariant

By

Ethan Alwaise

Master of Science

Mathematics

Ken Ono

Advisor

Matthew Weinschenk

Committee Member

David Zureick-Brown

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

An Algorithm for Numerically Computing Preimages of the j-invariant

By

Ethan Alwaise

Advisor: Ken Ono, Ph.D.

An abstract of

A thesis submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Master of Science

in Mathematics

2017

Abstract

An Algorithm for Numerically Computing Preimages of the j-invariant

By Ethan Alwaise

Here we explore the problem of numerically computing preimages of the j-invariant. We present an algorithm based on studying the asymptotics of the Fourier coefficients of the logarithmic derivative of $j(\tau)$. We use recent work of Bringmann, Kane, Löbrich, Ono, and Rolen, which gives asymptotics for the Fourier coefficients of divisor modular forms, to identify the real and imaginary parts of the preimage.

An Algorithm for Numerically Computing Preimages of the j-invariant

By

Ethan Alwaise

Advisor: Ken Ono, Ph.D.

A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Science
in Mathematics
2017

Acknowledgements

First, I would like to thank Ken Ono for serving as my advisor and an inspirational mentor over the past four years. Second, I would like to thank David Zureick-Brown for serving as my committee member and for offering indispensable advice and support over the past three years. Third, I would like to thank Matthew Weinschenk for serving as my committee member and as a personal role model. Lastly, I would also like to acknowledge John Duncan and David Zureick-Brown for providing helpful technical advice.

List of Figures

Table of Contents

Chapter 1

Introduction and Statement of Results

The theory of Diophantine equations is the branch of number theory concerned with finding integer or rational solutions to polynomial equations. The famous Fermat's last theorem, first conjectured by Pierre de Fermat in 1637, states that the Diophantine equation

$$x^n + y^n = z^n$$

has no nonzero rational solutions if $n \geq 3$. The problem remained open until finally a proof was given by Andrew Wiles and Richard Taylor in 1995.

Descartes' introduction of coordinate geometry in the 17th century opened the door for algebraic problems to be viewed geometrically. For instance, the real solutions to the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 = 0$$

form a curve in the xy plane called an ellipse. In general, if $f(x, y)$ is a degree

n polynomial in two variables, then the set of real solutions to the equation $f(x, y) = 0$ is called an **algebraic curve of degree** n. An algebraic curve is called **singular** if there exists a point on the curve at which both partial derivatives of the defining polynomial $f(x, y)$ vanish.

As in the case with Fermat's last theorem, we are often interested in finding rational points on an algebraic curve with rational coefficients. When $n = 1$, we have a linear equation

$$ay + bx + c = 0,$$

and the rational solutions are found easily using elementary algebra. When $n = 2$, we have an equation of the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

and we call the corresponding algebraic curve a conic. In this case, the rational points on the curve can be parametrized by projecting from a given rational point $\mathcal{O}$. More specifically, one uses a line L_0 with rational coefficients and draws the line L through $\mathcal{O}$ and Q for each point Q on L_0. A line intersects a conic at two points, counted with multiplicity, so for each point Q we obtain a point on the conic by taking the other point of intersection between the conic and L. Conversely, given a point P on the conic, we obtain a point L_0 by drawing the line connecting $\mathcal{O}$ and P and intersecting it with L_0. We thus obtain a one-to-one correspondence between points on the conic besides $\mathcal{O}$ and points on the line L_0. Furthermore, if the point P is rational, then since $\mathcal{O}$ is rational and L_0 has rational coefficients, the intersection point Q must be rational. Conversely, if the point Q is rational, then since $\mathcal{O}$ is rational and the conic has rational coefficients, the point P must also be rational. We thus obtain a one-to-one-correspondence between rational points on the conic besides $\mathcal{O}$ and rational points on L_0, the latter of which are easily described in terms of rational values of a single parameter.

We present an example by parametrizing the rational points on the circle

$$x^2 + y^2 = 1,$$

illustrated below:

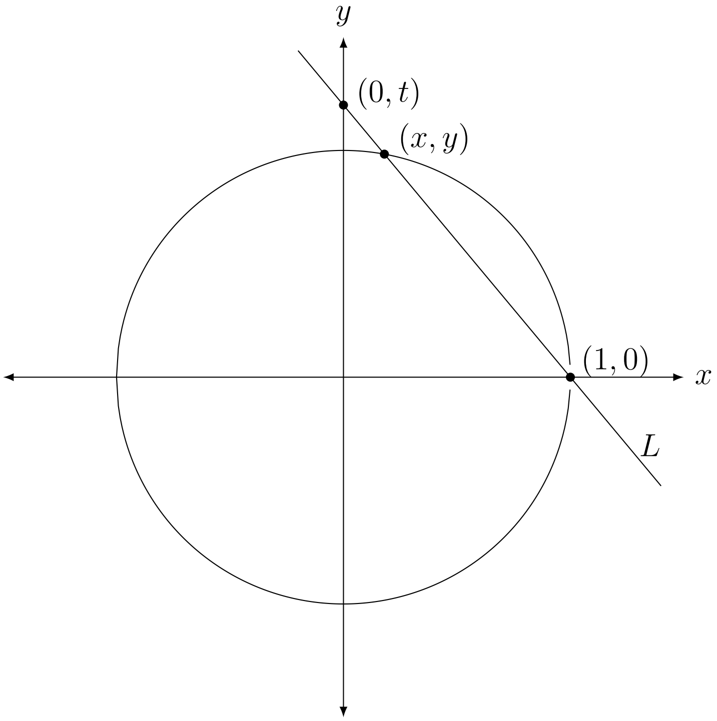

Figure 1.0.1: Rational Parametrization of $x^2 + y^2 = 1$

We will project from the point $(1,0)$ to the y-axis (see Figure 1.0.1). The line connecting $(1,0)$ and a point $(0,t)$ on the y-axis is $y = t(1-x)$. Substituting this equation into the equation for the circle and rearranging, we obtain the equation

$$t^2(1-x)^2 = 1 - x^2.$$

Cancelling a factor of $1 - x$ on both sides reduces the equation to

$$t^2(1-x) = 1 + x.$$

Solving for x in terms of t and then substituting the solution into the equation $y = t(1-x)$ gives

$$x = \frac{t^2-1}{t^2+1}, \qquad y = \frac{2t}{t^2+1}.$$

The point $(1,0)$ together with the points (x,y) as t ranges over $\mathbb{Q}$ give all rational points on the circle.

In this paper, we will be interested in the case $n = 3$, that is curves of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

A geometric principle similar to the one applied to the conics is at play here. Namely, given two rational points on a cubic, the line drawn between them will intersect the cubic in a third point which must also be rational. This principle hints at the following composition law. Given two rational points P and Q on a cubic, we define the point $P * Q$ to be third point of intersection between the cubic and the line between P and Q (see Figure 1.0.2).

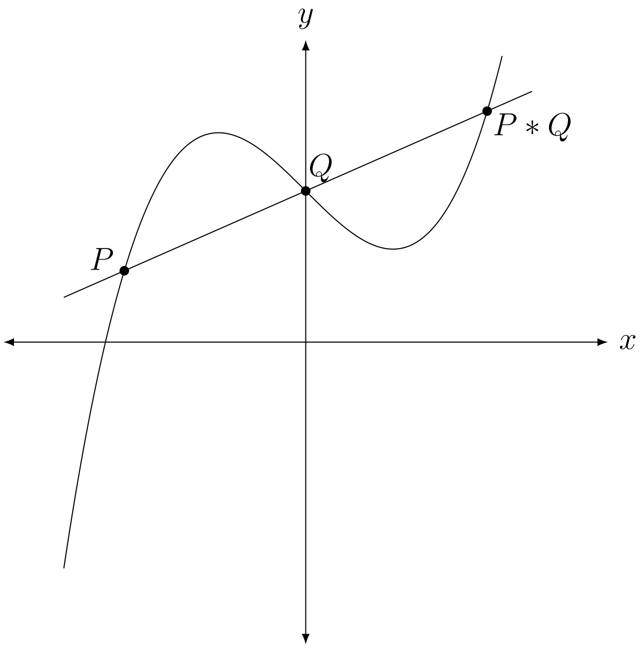

Figure 1.0.2: Composition of Points on a Cubic

By adding an additional step one can use this composition law to define a group law on the rational points of the cubic where the given rational point $\mathcal{O}$ is the identity. The group operation, which we denote by $+$, is given as follows. Given two rational points P and Q, we define $P + Q$ to be the third intersection point of the cubic and the line between $\mathcal{O}$ and $P * Q$, that is $P + Q = \mathcal{O} * (P * Q)$ (See Figure 1.0.5).

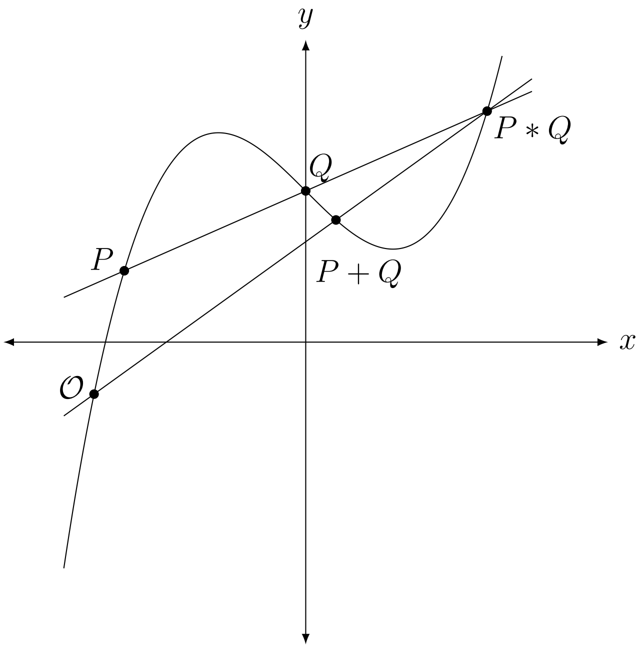

Figure 1.0.3: Group Law Defined on a Cubic

As suggested by the notation +, this operation is commutative. We remark that there are some additional subtleties which we have glossed over. If the line through P and Q is tangent to the the cubic at P, then we interpret $P * Q$ as P. To add P to itself, we take $P * P$ to be P. To put everything on a rigorous foundation, we must work in projective space with the homogenized cubic

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3 = 0.$$

The projective plane contains extra points at infinity which allow us to deal with the technical difficulties previously described.

The details of verifying that the set of rational points on a cubic is a group under + are given in [7]. The addition of points can be described purely in terms of algebraic formulas which hold over any given field. We thus obtain the following theorem:

The aforementioned algebraic formulas can be greatly simplified by working with a special form of the cubic known as **Weierstrass normal form**. A cubic in Weierstrass form has the form

$$y^2 = f(x) = 4x^3 - g_2x - g_3.$$

The above is the classical Weierstrass form. We shall also say that a cubic of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

is in Weierstrass form. A simple change of coordinate eliminates the x^2 term, and over $\mathbb{C}$ the transformation $x \to \sqrt[3]{4}x$ can be used to making the leading coefficient 4. Any cubic with a rational point can be put in Weierstrass form. One begins by homogenizing the cubic and then performing a projective transformation which makes a point at infinity the identity element of the group. The cubic is then dehomogenized and further coordinate changes are used to obtain a cubic in Weierstrass form. The key is that each of these transformations gives a bijection between rational points on the starting curving and rational points on the resulting curve and yields an isomorphism of the group laws. The details of these transformations can be found in [7].

We will work out an example offered as an exercise in [7] for the sake of clarity. Consider the cubic

$$v^2 - v - u^3 + u^2 = 0.$$

Setting $u = U/W$ and $v = V/W$ gives us the homogenous cubic

$$V^2W - VW^2 - U^3 + U^2W = 0,$$

from which we observe the rational point $P = [1, 0, 1]$. We will perform a change of coordinates in the projective plane that gives a one-to-one correspondence between the rational points of our starting curve and the new curve that will result. We begin by taking the line tangent to the cubic at P to be the axis $Z = 0$ in our new coordinate system. The tangent line at P is

$$-U - V + W = 0,$$

thus we set $Z = -U - V + W$. The next step is to intersect the tangent line to P with the cubic to obtain another rational point Q. We then take the line tangent to the cubic Q to be the axis $X = 0$. We substitute $V = W - U$ into the homogenized cubic equation to obtain the equation

$$(W - U)^2 W - (W - U)W^2 - U^3 + U^2 W = 0.$$

After simplifying we arrive at the equation

$$-U(W - U)^2 = 0,$$

thus $Q = [0, 1, 1]$. The tangent line at Q is

$$V - W = 0,$$

thus we take $X = V - W$. The last step is to choose as the axis $Y = 0$ some line through P other than the line $Z = 0$. We will use the line

$$-U + W = 0,$$

thus we take $Y = -U + W$. The change of coordinates $(U, V, W) \to (X, Y, Z)$

is the linear transformation

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ -1 & -1 & 0 \end{pmatrix} \begin{pmatrix} U \\ V \\ W \end{pmatrix}.$$

The matrix above is invertible, and so it is clear we have a one-to-one correspondence between the rational points of the curve in the coordinates U, V, W and our new curve in the coordinates X, Y, Z. Inverting the transformation, we find that

$$U = -X - Z,$$

$$V = Y - Z,$$

$$W = -X + Y - Z.$$

We substitute into our cubic to obtain the cubic

$$(Y-Z)^2(-X+Y-Z)-(Y-Z)(-X+Y-Z)^2-(-X-Z)^3+(-X-Z)^2(-X+Y-Z) = 0.$$

After simplifying, we arrive at the equation

$$XY^2 + X^2Z + XZ^2 + YZ^2 = 0.$$

Setting $X = xZ$ and $Y = yZ$ gives us the nonhomogenous cubic

$$xy^2 + x^2 + x + y = 0.$$

Multiplying through by x gives us

$$x^2y^2 + x^3 + x^2 + xy = 0.$$

We rename the variable xy as y to arrive at the equation

$$y^2 + y + x^3 + x^2 = 0.$$

Completing the square in y gives us

$$\left(y - \frac{1}{2}y\right)^2 + x^3 + x^2 - \frac{1}{4} = 0.$$

Finally, replacing $y - \frac{1}{2}y$ by y gives us the Weierstrass curve

$$y^2 = -x^3 - x^2 + \frac{1}{4}.$$

We now explain the virtues of putting a cubic into Weierstrass form. Consider the equation

$$y^2 = x^3 + ax^2 + bx + c.$$

The homogenous cubic is

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Setting $Z = 0$ gives the equation $X^3 = 0$, which has a triple root at $X = 0$, thus the cubic meets the line $Z = 0$ at infinity three times, but at the same point. Thus a cubic in Weierstrass form has exactly one point at infinity, which we denote by $\mathcal{O}$. The point $\mathcal{O}$ is the point at which vertical lines meet. Taking $\mathcal{O}$ to the identity in the group law resolves the technical difficulties we saw in defining the group law, as now every line intersects the cubic in three points. A vertical line intersects the cubic at two points in the xy plane and at the point $\mathcal{O}$. One of the main conveniences of the Weierstrass form is that the negative of a point is given simply by negating its x-coordinate. If

$P = (x, y)$ is a point on a Weierstrass curve, then so is $Q = (x. - y)$. The line connecting P and Q is vertical and intersects the cubic again at the point $\mathcal{O}$ at infinity. Joining $\mathcal{O}$ to $\mathcal{O}$ to form the line $Z = 0$ at infinity and taking the third intersection point gives $\mathcal{O}$ again, since the cubic meets the point $\mathcal{O}$ with multiplicity three. Therefore $P = -Q$.

We will work out a specific example to illustrate the addition of points. Consider the Weierstrass curve

$$y^2 = x^3 + 1,$$

illustrated below:

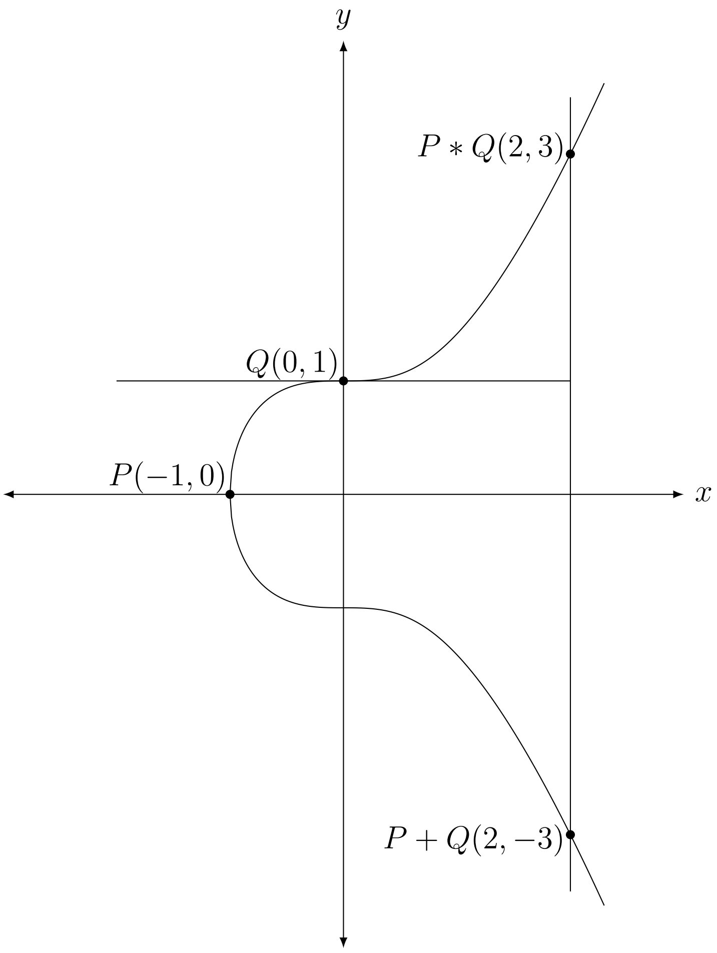

Figure 1.0.4: Addition of Points on $y^2 = x^3 + 1$

We will compute the sum of the points $P = (-1, 0)$ and $Q = (0, 1)$. The line joining P and Q is $y = x + 1$. We substitute into the cubic to obtain

$$(x + 1)^2 = x^3 + 1.$$

Expanding the left-hand side and putting everything on one side gives the equation

$$x^3 - x^2 - 2x = 0.$$

Since P and Q are points on the cubic and the line $y = x$, the above cubic has roots at $x = -1$ and $x = 0$. We factor the above cubic as

$$x(x + 1)(x - 2) = 0,$$

thus the x-coordinate of the third intersection point $P * Q$ is $x = 2$. Substituting into the line $y = x + 1$ gives us that $P * Q = (2, 3)$. We draw the vertical line through $P * Q$ to connect $P * Q$ to $\mathcal{O}$. The third point of intersection is $(2, -3)$, thus $P + Q = (2, -3)$ (see Figure 1.0.5).

We will also compute the point $2Q$. The line joining Q to Q is the line tangent to the cubic at Q. We differentiate our curve implicitly to find that

$$\frac{dy}{dx} = \frac{3x^2}{2y} = \frac{3x^2}{2x^3 + 2}.$$

Plugging the x-coordinate of Q into the above formula, we find that the slope of the tangent line is 0. Thus the tangent line is $y = 1$. Substituting into the cubic, we obtain the equation

$$x^3 + 1 = 1,$$

thus $Q * Q = Q$. Joining Q to $\mathcal{O}$ and taking the third point of intersection, we find that $2Q = (0, -1)$. We remark that $(0, -1) = -Q$, hence $2Q = -Q$, i.e., Q is a point of order 3.

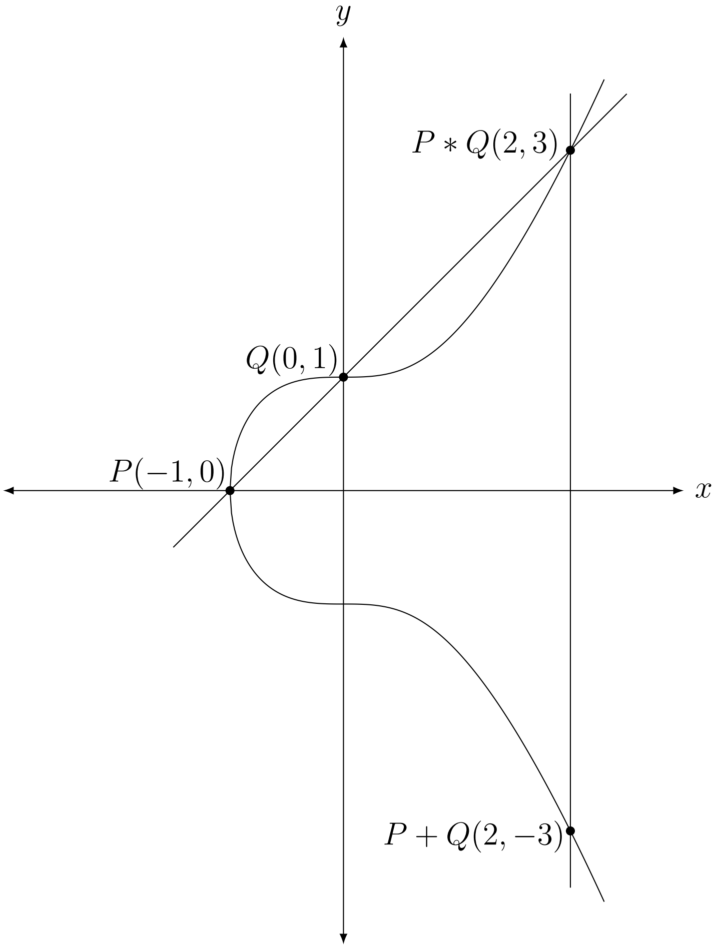

Figure 1.0.5: Addition of Points on $y^2 = x^3 + 1$

A nonsingular cubic curve is called an **elliptic curve**. For a Weierstrass curve $y^2 = f(x)$, this is equivalent to the condition that the complex roots of $f(x)$ are distinct. The theory of elliptic curves is an active area of modern research in number theory. The algebraic formula which describe the addition of points on a cubic hold in any field. We thus obtain the following theorem:

Theorem 1.0.1. *For a field F, the set of points in F on a cubic over F form a group under $+$. We denote this group by $E(F)$.*

Elliptic curves over $\mathbb{C}$ arise from the classical theory of elliptic functions. Over finite fields, elliptic curves exhibit interesting properties which offer applications to cryptography and are the basis of the elliptic curve factorization method. Of particular interest are elliptic curves defined over $\mathbb{Q}$. A famous result known as the Mordell-Weil theorem guarantees that the group of rational points on an elliptic curve is always finitely generated. Moreover, a theorem due to Mazur gives the complete list of possible torsion subgroups. As an example, the group of rational points on the elliptic curve

$$y^2 = x^3 - x$$

over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, corresponding to three points of order 2 and the identity. The elliptic curve

$$y^2 = x^3 - 7x + 10$$

is an example of an elliptic curve of rank 2. It is still an open problem whether or not elliptic curves can have arbitrarily large rank. It is difficult to produce elliptic curves with large rank. Indeed, it is conjectured that 100% of elliptic curves have rank 0 or 1. The largest exactly known rank of an elliptic curve is 19. Curves of rank at least 28 are known, but their exact ranks are not known.

Although the Mordell-Weil theorem guarantees that the group of rational points on an elliptic curve is always finitely generated, there still is no known algorithm for computing the rank of $E(\mathbb{Q})$. The Birch and Swinnerton-Dyer conjecture, first conjectured in 1965, offers a numerical method of calculating ranks. Namely, the rank of $E(\mathbb{Q})$ is conjectured to be the order of the zero at $s = 1$ of the associated Hasse-Weil L-function $L(E, s)$. The conjecture is one of the seven Millennium Prize Problems listed by the Clay Mathematics

Institute.

The term elliptic curve is somewhat curious, as elliptic curves are not ellipses. The name stems from the fact that elliptic curves originally arose from the problem of determining the arc length of an ellipse. If $Q \in \mathbb{C}[x]$ is a polynomial of degree at most 4 and $F(x, y)$ is rational in x and $y = \sqrt{Q(x)}$, then the integral

$$\int F(x, y)dx$$

is called an **elliptic integral** if is not elementary. The name elliptic stems from the fact that the arc length of an ellipse (see Figure 1.0.6) is given by an elliptic integral.

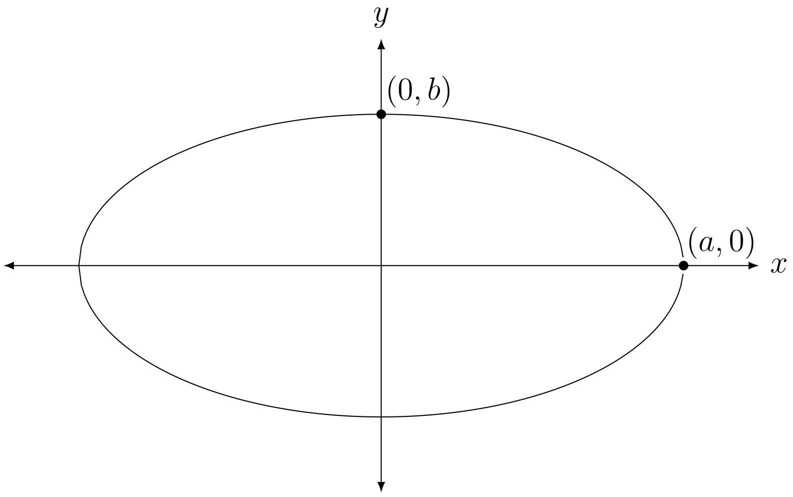

Figure 1.0.6: The Ellipse $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$

We will work out the integral giving the arc length L of the ellipse

$$\frac{1}{4}x^2 + y^2 = 1.$$

We parametrize the ellipse as

$$x = 2\cos\theta, \qquad y = \sin\theta,$$

where $0 \leq \theta \leq 2\pi$. Using the symmetry of the ellipse about both axes, we have

$$L = 4\int_0^{\pi/2} \sqrt{4\sin^2\theta + \cos^2\theta d\theta}.$$

Replacing $\sin^2\theta$ with $1-\cos^2\theta$ and factoring out 4 from inside the square root, we obtain

$$L = 8\int_0^{\pi/2} \sqrt{1 - \frac{3}{4}\cos^2\theta d\theta}.$$

Now we make the substitution $t = \cos\theta$ to obtain

$$L = 8\int_0^1 \sqrt{\frac{1-\frac{3}{4}t^2}{1-t^2}}dt.$$

We see that the integral above is elliptic. In general, the arc length of an ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad (a > b)$$

is given by $4aE(k)$, where $k = \sqrt{1 - \dfrac{b^2}{a^2}}$ and

$$E(k) = \int_0^1 \sqrt{\frac{1-k^2t^2}{1-t^2}}dt$$

is Jacobi's **complete elliptic integral of the second kind**.

Gauss and Abel discovered that the inverse of functions of the form

$$f(x) = \int_0^x F(x,y)dx,$$

where the integral on the right-hand side is elliptic, belong to an **elliptic function** field. An elliptic function is a meromorphic function with two $\mathbb{R}$-linearly independent periods ω_1 and ω_2. Such a function is naturally defined on the complex torus $\mathbb{C}/\Lambda$, where Λ is the $\mathbb{Z}$-lattice generated by the two periods. Periodicity implies that the sum of the residues of an elliptic function in any period parallelogram must be 0. Periodicity and Liouville's theorem imply that an elliptic function must have at least one pole, hence an elliptic function has at least two poles, counted with multiplicity. Armed with this information, one naively tries to construct an elliptic function by considering a sum over the period lattice

$$\sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^2}.$$

Unfortunately, the above series diverges. However, the idea can be salvaged by taking the integral

$$\frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

The above function is known as the **Weierstrass $\wp$-function**. It is an elliptic function with periods $\omega \in \Lambda$ analytic except for an order 2 pole at each $\omega \in \Lambda$. Near the origin, the Laurent series for $\wp(z)$ is given in terms of the **invariants** $g_2 = 60G_4$ and $g_3 = 140G_2$. Here G_n denotes the **Eisenstein series of weight** n

$$\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^n} \qquad (n \geq 3).$$

Forming linear combinations of the Laurent expansions of $\wp$ and $\wp'$ shows that the $\wp$-function satisfies the differential equation

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3. \tag{1.0.1}$$

Considering a contour integral over a period parallelograms and using the fact that $\wp$ has exactly three poles inside any period parallelogram, one can show that the roots e_1, e_2, e_3 of the cubic on the right-hand side are distinct. Moreover, the e_i are the values of $\wp$ at the half periods, i.e.,

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), \qquad e_2 = \wp\left(\frac{\omega_2}{2}\right), \qquad e_3 = \wp\left(\frac{\omega_1 + \omega_2}{2}\right).$$

The differential equation satisfied by $\wp$ is a cubic in Weierstrass form, giving a clear connection between the $\wp$-function and elliptic curves. The map

$$z \to [1 : \wp(z) : \wp'(z)]$$

gives a group isomorphism of the torus $\mathbb{C}/\Lambda$ with the abelian group structure defined on the projective cubic

$$y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3.$$

Given a Weierstrass cubic $y^2 = 4x^3 - g_2 x - g_3$ defining an elliptic curve $E(\mathbb{C})$, it is natural to ask for an isomorphic torus $\mathbb{C}/\Lambda$. This question is answered for elliptic curves with real roots by the following theorem:

Theorem 1.0.2. *Let $y^2 = 4x^3 + ax + b$ be an equation defining an elliptic curve E over $\mathbb{C}$ with real roots $e_1 < e_2 < e_3$. Then E can be realized as the period lattice generated by the periods*

$$\omega_1 = \int_{\infty}^{e_1} \frac{dw}{\sqrt{(w - e_1)(w - e_2)(w - e_3)}},$$
$$\omega_2 = \int_{\infty}^{e_2} \frac{dw}{\sqrt{(w - e_1)(w - e_2)(w - e_3)}},$$

where e_1, e_2, e_3 are the roots of the equation defining E.

Proof. See Theorem 3.1.1 in Chapter 3. □

A similar theory exists for elliptic curves with general complex roots. The problem of finding a torus model for an elliptic curve $E(\mathbb{C})$ with real roots thus comes down to computation of the integral

$$\int_\gamma \frac{dz}{\sqrt{(z-e_1)(z-e_2)(z-e_3)}}.$$

Through suitable transformations, the above integral can be put in the form

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

Gauss made the remarkable discovery that $I(a,b)$ is unchanged if a and b are replaced with their arithmetic mean and geometric mean, respectively. Iterative replacemement and passing to the limit shows that $I(a,b)$ is given in terms of the **arithmetic-geometric mean** $M(a,b)$. Elementary manipulations show that $I(a,b)$ can be rewritten in terms of the **complete elliptic integral of the first kind**

$$K(k) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}.$$

Using the binomial theorem to rewrite the integrand and integrating term by term shows that

$$K(k) = \frac{\pi}{2}\sum_{n=0}^{\infty}\left[\frac{(2n-1)!!}{(2n)!!}\right]^2 k^{2n}.$$

The series on the right-hand side is a value of the **Gaussian hypergeometric series**

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

The hypergeometric series thus gives a way of numerically finding the periods ω_1 and ω_2.

Given an elliptic curve $E(\mathbb{C})$ defined by a cubic $y^2 = 4x^3 - g_2x - g_3$, we define its j**-invariant** to be

$$j = \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

This importance of this numerical statistic comes from the following theorem:

Theorem 1.0.3. *Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if they have the same j-invariant.*

Proof. See Theorem 3.2.9 in Section 3.2. □

The definition of the Eisenstein series shows that g_2 and g_3 are homogenous functions of ω_1 and ω_2 of degrees -4 and -6, respectively. It follows that j, considered as a function of ω_1 and ω_2, is homogenous of degree 0. Therefore

$$j(\omega_1, \omega_2) = j(1, \omega_2/\omega_1).$$

We let $\tau = \omega_2/\omega_1$ and label the ω_i such that $\mathrm{Im}(\tau) > 0$. We may thus consider $j(\tau)$ as a function of one complex variable in the upper half-plane $\mathbb{H}$. The function $j(\tau)$ is called **Klein's modular function**. It is easy to show that $j(\tau)$ is invariant under the action

$$\tau \to \frac{a\tau + b}{c\tau + d},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, i.e., j is a **modular function** on the **modular group** $\mathrm{SL}_2(\mathbb{Z})$, analytic on $\mathbb{H}$ with a single simple pole at the cusp ∞. The j function plays many important roles in number theory. Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if they have the same j-invariant, thus j parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$. Special values of j

generate maximal abelian extensions of imaginary quadratic fields. Monstrous moonshine tells us that its Fourier coefficients turn out to be the graded dimensions of representations of the monster group.

Considered as a function from $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ to $\mathbb{C}$, j is a bijective function. Given a complex number α, we would like to be able to produce $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ such that $j(\tau) = \alpha$. The method due to Gauss for evaluating period integrals offers a solution to this problem. Given a complex number α, one easily produces an elliptic curve $E(\mathbb{C})$ whose j-invariant is α. One then computes the period integrals giving ω_1 and ω_2 using Gauss' hypergeometric evaluation. Then j evaluated at the ratio ω_2/ω_1 is equal to α. One may then find an appropriate sequence of $\mathrm{SL}_2(\mathbb{Z})$ transformations to find the desired τ.

A natural problem is to invert j without making use of a model of an elliptic curve. To this end, we shall offer an efficient numerical algorithm which makes use of the theory of polar harmonic Maass forms. The algorithm is based in recent work of Bringmann et al., which gives a method for computing divisors of modular forms. The idea stems from the fact that the logarithmic derivative

$$\frac{j'(\tau)}{j(\tau) - \alpha}$$

is a weight 2 modular form on $\mathrm{SL}_2(\mathbb{Z})$ with a single simple pole at the unique point $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ such that $j(\tau) = \alpha$. In [5], the authors obtain asymptotics for the Fourier coefficients of

$$H_z(\tau) = -\frac{1}{2\pi i}\frac{j'(\tau)}{j(\tau) - j(z)},$$

which we will use to numerically calculate the simple pole of $H_z(\tau)$. Our main result is stated in the following following theorem.

Theorem 1.0.4. *Let $\alpha \in \mathbb{C}$ and let $z \in SL_2(\mathbb{Z})\backslash\mathbb{H}$ such that $j(z) = \alpha$. Let*

$$H_z(\tau) = -\frac{1}{2\pi i}\frac{j'(\tau)}{j(\tau) - \alpha} = \sum_{n=0}^{\infty} a(n)q^n.$$

Write $z = x + iy$. Then y is given by

$$y = \lim_{n\to\infty} b(n), \qquad \textit{where } b(n) = \frac{\log|a(n)|}{2\pi n}.$$

For the computation of x, we have three cases. If $\alpha = 0$, then $x = -\frac{1}{2}$. If $\alpha \neq 0$, let

$$c(n) = \begin{cases} \mathrm{Re}(a(n))e^{-2\pi ny} & \textit{if } \lim_{n\to\infty}|a(n)|e^{-2\pi ny} = 1, \\ \frac{1}{2}a(n)e^{-2\pi ny} & \textit{otherwise.} \end{cases}$$

Let $w_n = \cos^{-1}(c(n))$. Then an approximation for x is given by one of

$$x \approx \pm\frac{1}{2\pi}(w_n \pm w_{n-1})$$

or

$$x \approx \pm\frac{1}{2\pi}(w_n + w_{n-1} - 2\pi).$$

for sufficiently large n. The correct value of x can be determined by substituting back into the asymptotic formula.

Proof. See Chapter 4. □

This thesis is organized as follows. In Chapter 2, we review the basic theory of elliptic functions and introduce the $\wp$ function. We give the differential equation $\wp$ satisfies and explain how to produce a torus isomorphic to a given elliptic curve $E(\mathbb{C})$ by evaluating period integrals using the method stemming from Gauss. We introduce Klein's modular function j and explain how the inverse problem can be solved using Gauss' hypergeometric evaluation. In Chapter 3 we recall the basic facts about modular forms and harmonic Maass forms that we will be using. In Chapter 4, we prove Theorem 1.0.4 and conclude with some numerical examples of the result.

Chapter 2

Preliminaries on Elliptic Curves over $\mathbb{C}$

In this chapter we will recall some of the basic properties of elliptic functions and introduce the $\wp$-function. We will give the differential equation satisfied by $\wp$ and show how to realize an elliptic curve $E(\mathbb{C})$ as a complex torus using Gauss' hypergeometric evaluation. We also introduce Klein's modular function j, review some of its basic properties, and discuss the inverse problem. We closely follow [1] in our treatment of this material.

2.1 Elliptic Functions and the Weierstrass $\wp$ Function

Here we gather some basic facts about elliptic functions and define the Weierstrass $\wp$ function. Recall that a function f is called periodic with period ω if $f(z+\omega) = f(z)$ whenever z and $z+\omega$ are in the domain of f. If ω_1 and ω_2 are two periods of f, then so is $m\omega_1 + n\omega_2$ for any integers m and n. If f has two periods ω_1 and ω_2 whose ratio ω_2/ω_1 is not real, then f is called doubly periodic. We denote by $\Omega(\omega_1, \omega_2)$ the lattice $\{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ generated by ω_1 and ω_2. If ω_1 and ω_2 are clear, we simply write Ω. We say that two periods ω_1 and ω_2 constitute a fundamental pair of periods if $\Omega(\omega_1, \omega_2)$ contains every period of f. The following lemma gives a necessary and sufficient condition for two periods to constitute a fundamental pair.

Lemma 2.1.1. *A pair of periods $\{\omega_1, \omega_2\}$ is fundamental if and only if the triangle with vertices $0, \omega_1, \omega_2$ contains no other periods in its interior or on its boundary.*

Proof. Suppose that $\{\omega_1, \omega_2\}$ is a fundamental pair of periods. Each point in the parallelogram with vertices $0, \omega, \omega_1, \omega_1 + \omega_2$ is of the form $\alpha\omega_1 + \beta\omega_2$ with $0 \leq \alpha, \beta \leq 1$. Among these points only the vertices are periods, since $\{\omega_1, \omega_2\}$ is fundamental.

Conversely, suppose that the triangle with vertices $0, \omega_1, \omega_2$ contains no other periods in its interior or on its boundary. Since ω_2/ω_1 is not real, ω_1 and ω_2 span $\mathbb{C}$ over $\mathbb{R}$. Then any period ω can be written in the form $\omega = c_1\omega_1 + c_2\omega_2$ for some real numbers c_1 and c_2. Let $r_1 = c_1 - \lfloor c_1 \rfloor$ and $r_2 = c_2 - \lfloor c_2 \lfloor$, where $\{x\}$ denotes the fractional part of x. Now $0 \leq r_1, r_2 < 1$ and $\omega' = r_1\omega_1 + r_2\omega_2$ is also a period since it is contained in $\Omega(\omega_1, \omega_2)$. If one of r_1 or r_2 is nonzero, then ω' is a period lying inside the parallelogram with vertices $0, \omega_1, \omega_2, \omega_1 + \omega_2$. But then either ω' or $\omega_1 + \omega_2 - \omega$ lies inside the triangle with vertices $0, \omega_1, \omega_2$ or on its boundary, contradicting the hypothesis. □

We now given equivalent condition for two pairs of periods to generate the same lattice.

Proposition 2.1.2. *Let $\{\omega_1, \omega_2\}$ and $\{\omega_1, \omega_2\}$ be pairs of periods. Then $\Omega(\omega_1, \omega_2) = \Omega(\omega_1', \omega_2')$ if and only if there exist integers a, b, c, d with $ad - bc =$*

±1 *such that*

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

Proof. The pairs $\{\omega_1, \omega_2\}$ and $\{\omega_1, \omega_2\}$ generate the same lattice if and only if each member of either pair can be expressed as a $\mathbb{Z}$-linear combination of the members of the other pair. This is equivalent to the existence of an invertible linear transformation over $\mathbb{Z}$ taking (ω_1, ω_2) to (ω_1', ω_2'). To finish, recall that a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer coefficients is invertible over $\mathbb{Z}$ if and only if $ad - bc = \pm 1$. □

We now define the main object of study in this section.

Definition 2.1.3. An elliptic function is a doubly periodic function which is meromorphic.

We will show that any elliptic function which is not constant has a fundamental pair of periods. First we require the following lemma, which states that the periods of an analytic function must be discrete unless it is constant.

Lemma 2.1.4. *Let f be a function analytic on an open connected set D. Suppose there exists a convergent sequence of distinct periods $\{\omega_n\}_{n=1}^{\infty}$. Then f is constant on D.*

Proof. If $\{\omega_n\}_{n=1}^{\infty}$ is a convergent sequence of periods, then $\{\omega_{n+1} - \omega_n\}_{n=1}^{\infty}$ is a sequence of periods converging to 0. Pick a point $z \in D$. Since D is open and $\omega_n' = \omega_{n+1} - \omega_n$ tends to 0, by dropping finitely many of the ω_n', we may assume that $z + \omega_n' \in D$ for all $n \geq 1$. By periodicity, we have

$$\frac{f(z + \omega_n') - f(z)}{\omega_n'} = 0,$$

for all $n \geq 1$. Here we use distinctness to ensure that $\omega_n' \neq 0$. Taking the limit as $n \to \infty$ shows that $f'(z) = 0$. Therefore $f'(z) = 0$ for all $z \in D$, hence f is constant on D. □

We are now ready to prove the existence of fundamental periods.

Proposition 2.1.5. *A nonconstant elliptic function has a fundamental pair of periods.*

Proof. Let f be a nonconstant elliptic function. Choose a punctured disc centered at the origin in which f is analytic. By analytic continuation f is not constant on this disc. By Lemma 2.1.4 we may choose a period ω_1 lying in the disc with minimal absolute value R and minimal positive argument θ. If possible, choose a period ω_2 with absolute value R and minimal positive argument greater than θ. If not, choose a period ω_2 with minimal absolute value greater than R and minimal positive argument. The minimality conditions ensure that no other periods lie inside the triangle with vertices $0, \omega_1, \omega_2$. Therefore $\{\omega_1, \omega_2\}$ is a fundamental pair of periods by Lemma 3. □

In trying to construct a nonconstant elliptic function it is natural to consider sums over the period lattice, namely $\sum_{\Omega\setminus\{0\}} \omega^{-\alpha}$. The following lemma deals with the convergence of such a series:

Lemma 2.1.6. *If α is real the series*

$$\sum_{\omega\in\Omega\setminus\{0\}} \frac{1}{\omega^\alpha}$$

converges absolutely if and only if $\alpha > 2$.

Proof. Assume without loss of generality that $|\omega_1| \leq |\omega_2|$. Let $r = |\omega_1|$ and $R = |\omega_1 + \omega_2|$. For each $n \geq 1$ let W_n be the set of periods on the parallelogram with vertices $\pm n\omega_1 \pm n\omega_2$. We have $|W_n| = 8n$ and $nr \leq |\omega| \leq nR$ for $\omega \in W_n$. The set of nonzero periods is equal to the union of the W_n. If we denote by $S(n)$ the sum $\sum |\omega|^{-\alpha}$ taken over all $\omega \in W_k$ for $k \leq n$, we have

$$\sum_{k=1}^{n} \frac{8k}{(kR)^\alpha} \leq S(n) \leq \sum_{k=1}^{n} \frac{8k}{(kr)^\alpha}$$
$$\frac{8}{R^\alpha} \sum_{k=1}^{n} \frac{1}{k^{\alpha-1}} \leq S(n) \leq \frac{8}{r^\alpha} \sum_{k=1}^{n} \frac{1}{k^{\alpha-1}}.$$

The lemma now follows since the series $\sum_{k=1}^{\infty} 1/k^{\alpha-1}$ converges if and only if $\alpha > 2$. □

The following lemma will be crucial in proving the analyticity of the $\wp$ function.

Lemma 2.1.7. *If $\alpha > 2$ and $R > 0$ the series*

$$\sum_{\substack{\omega \in \Omega \\ |\omega| > R}} \frac{1}{(z-\omega)^\alpha}$$

converges absolutely and uniformly in the disk $|z| \leq R$.

Proof. Let c be the minimum of $|\omega|$ for all $\omega \in \Omega$ with $|\omega| > R$. For z with $|z| \leq R$ we have

$$\left|\frac{z-\omega}{\omega}\right| = \left|1 - \frac{z}{\omega}\right| \geq 1 - \left|\frac{z}{\omega}\right| \geq 1 - \frac{R}{R+c} = M.$$

Then if $\alpha \geq 1$ we have

$$\frac{|\omega|^\alpha}{|z-\omega|^\alpha} \leq \frac{1}{M^\alpha}$$
$$\frac{1}{|z-\omega|^\alpha} \leq \frac{1}{M^\alpha |\omega|^\alpha}.$$

Since M depends only on R, the proof is complete by Lemma 2.1.6. □

Definition 2.1.8. Let ω_1 and ω_2 be complex numbers whose ratio ω_2/ω_1 is not real. The Weierstrass $\wp$ function is defined as

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

where Ω is the lattice $\{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$.

The following theorem gives our first example of an elliptic function. The function in question is in fact the derivative of $\wp'$, as we will later show, and its periodicity will be used to prove the periodicity of $\wp$.

Theorem 2.1.9. *The function*

$$f(z) = \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3}$$

is an elliptic function with periods ω_1, ω_2 with a pole of order 3 at each period.

Proof. By Lemma 2.1.6, the sum defining f converges uniformly in any compact disk $|z| \leq R$ if we exclude the finitely many periods ω lying inside the disk, hence f is analytic in the disk. The remaining terms are also analytic except for a pole of order 3 at each period. Next we show that f has periods ω_1, ω_2. We have

$$f(z+\omega_1) = \sum_{\omega \in \Omega} \frac{1}{(z-(\omega-\omega_1))^3}.$$

As ω runs through all periods in Ω, so does $\omega - \omega_1$, hence the above series is a rearrangement of the series defining f. By absolute convergence, it follows that $f(z+\omega_1) = f(z)$. Similarly $f(z+\omega_2) = f(z)$, thus completing the proof. □

We are now ready to show that $\wp$ is indeed an elliptic function.

Theorem 2.1.10. *The Weierstrass $\wp$ function is an elliptic with periods ω_1 and ω_2 and poles of order 2 at the lattice points. Moreover $\wp$ is an even function of z.*

Proof. By Lemma 2.1.7, given a compact disk $|z| \leq R$, there exists a constant M such that

$$\frac{1}{|z-\omega|^2} \leq \frac{M}{|\omega|^\alpha}$$

for all periods ω with $|\omega| > R$. For such periods we have the estimate

$$\left|\frac{z(2\omega - z)}{(z-\omega)^2\omega^2}\right| \leq \frac{1}{|z-\omega|^2}\frac{3|z||\omega|}{|\omega|^2} \leq \frac{3MR}{|\omega|^3}.$$

If we exclude the finitely many periods lying inside the disk $|\omega| \leq R$, the sum $\sum_{\omega\in\Omega} |\omega|^{-3}$ converges by Lemma 2.1.6. Therefore, excluding such periods, the series defining $\wp$ converges absolutely and uniformly in the compact disc $|z| \leq R$ and hence is analytic in this disk. The periods lying inside the disk give poles of order 2.

To see that $\wp$ is even, note that

$$(-z-\omega)^2 = (z+\omega)^2 = (z-(-\omega))^2.$$

As ω runs through all lattice points so does $-\omega$, hence $\wp(-z) = \wp(z)$.

It only remains to show that $\wp$ is elliptic. The derivative of $\wp$ is

$$\wp'(z) = -2\sum_{\omega\in\Omega}\frac{1}{(z-\omega)^3}.$$

By Theorem 2.1.9, $\wp'(z)$ is periodic, hence $\wp'(z+\omega) - \wp'(z) = 0$ for each period $\omega \in \Omega$. Therefore the function $\wp(z+\omega) - \wp(z)$ is constant. Setting $z = -\omega/2$ gives $\wp(\omega/2) - \wp(-\omega/2) = 0$, since $\wp$ is even, hence $\wp(z+\omega) - \wp(z) = 0$ for each period $\omega \in \Omega$. □

The next theorem shows that near the origin, $\wp$ has a Laurent series given in terms of the Eisenstein series, which we now define.

Definition 2.1.11. If $n \geq 3$ the **Eisenstein series of order** n is defined as

$$G_n = \sum_{\omega \neq 0} \frac{1}{\omega^n}.$$

We now obtain the aforementioned Laurent series expansion.

Theorem 2.1.12. *Let r be the minimum of $|\omega|$ among nonzero periods ω. Then for $0 < |z| < r$, we have*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2} z^{2n},$$

where

$$G_n = \sum_{\omega \neq 0} \frac{1}{\omega^n} \qquad \text{for } n \geq 3.$$

Proof. We have

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-z/\omega)^2} = \frac{1}{\omega^2} + \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n}$$

when $0 < |z| < r$, thus

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}}.$$

Summing over all ω and using absolute convergence we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\omega \neq 0} \frac{1}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) G_{n+2} z^n.$$

The theorem then follows by noting that all of the odd coefficients must vanish since $\wp$ is an even function. □

2.2 Differential Equation Satisfied by $\wp$

As we show in the following theorem, the Weierstrass $\wp$ function satisfies a nonlinear differential equation which defines an elliptic curve over $\mathbb{C}$.

Theorem 2.2.1. *The function $\wp$ satisfies the differential equation*

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

*where g_2 and g_2 are the **invariants** defined as*

$$g_2 = 60G_4, \qquad g_3 = 140G_6.$$

Proof. Using the Laurent series expansion given by Theorem 2.1.12, we find that

$$\wp'(z) = -\frac{2}{z^3} + 6_4 z + 20G_6 z^3 + \cdots$$

near $z = 0$. Squaring gives

$$(\wp'(z))^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \cdots,$$

We also have

$$4(\wp(z))^3 = \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + \cdots,$$

thus

$$(\wp'(z))^2 - 4\wp^3(z) + 60G_4\wp(z) = -140G_6 + \cdots.$$

The right-hand side is an analytic elliptic function, hence must have be the constant function equal to $-140G_6$ by Lemma 2.1.4. This proves the theorem. □

It turns out that we can factor the cubic $4\wp^3 - g_2\wp - g_3$ explicitly. We define the following special values of $\wp$.

Definition 2.2.2. We denote the values of $\wp$ at the half-periods by

$$e_1 = \wp\left(\frac{\omega_1}{2}\right), \quad e_2 = \wp\left(\frac{\omega_2}{2}\right), \quad e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right).$$

We will prove that the e_i are the roots of the cubic $4\wp^3 - g_2\wp - g_3$. First we require the following lemma.

Lemma 2.2.3. *If f is an elliptic function, then the number of zeros of f in any period parallelogram is equal to the number of poles of f, each counted with multiplicity.*

Proof. Let C be the boundary of such a parallelogram. We must show that

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = 0.$$

Now f'/f is elliptic with the same periods of f, hence the integrals along the parallel edges of C cancel. □

We now prove the aforementioned theorem.

Theorem 2.2.4. *We have*

$$4\wp^3(z) - g_2\wp(z) - g_3 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

Moreover, the roots e_1, e_2, e_3 are distinct, hence $g_2^3 - 27g_3^2 \neq 0$.

Proof. By periodicity we have $\wp'(-\omega/2) = \wp'(\omega - \omega/2) = \wp'(\omega/2)$. Since $\wp'$ is odd, we must have $\wp'(\omega/2) = 0$, hence the half-periods $\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$ are zeroes of $\wp'$. Shift the parallelogram with vertices $0, \omega_1, \omega_2, \omega_1+\omega_2$ so that the resulting parallelogram contains the half-periods but contains no poles of

$\wp'$ except 0. Since the pole at 0 is of order 3, the zeros at the half-periods must be simple by Lemma 2.2.3. Translating $\wp'$ appropriately shows that $\wp'$ contains no further zeros in the parallelogram with vertices $0, \omega_1, \omega_2, \omega_1 + \omega_2$. The differential equation shows that the half-periods are also zeros of the cubic $4\wp^3 - g_2\wp - g_3$, hence the claimed factorization holds.

Now we prove distinctness. The elliptic function $\wp - e_1$ has a double zero at $\omega_1/2$ since its derivative $\wp'$ has a simple zero at $\omega_1/2$. Similarly $\wp - e_2$ has a double zero at $\omega_2/2$. If $e_1 = e_2$, then $\wp - e_1$ has a double zero at ω_1 and at ω_2. By Lemma 2.2.3, this would imply that the orders of the poles of $\wp - e_1$ would sum to at least 4. But clearly this sum is 2, hence $e_1 \neq e_2$ and similarly $e_1 \neq e_3$ and $e_2 \neq e_3$. It follows that $g_2^3 - 27g_3^2$, the discriminant of the polynomial $4x^3 - g_2x - g_3$, is nonzero. □

Chapter 3

Determining Fundamental Periods from an Elliptic Curve over $\mathbb{C}$

3.1 Period Integrals

Given an Weierstrass cubic model for an elliptic curve E over $\mathbb{C}$, we would like to be able to produce a complex torus isomorphic to E. This amounts to finding periods ω_1, ω_2 such that the Weierstrass $\wp$ function with periods ω_1, ω_2 satisfies the differential equation described by the given cubic. In this chapter we address this question. The strategy is to assume that such a $\wp$ function exists, then use the differential equation satisfied by $\wp$ to show that the periods are given in terms of certain integrals. We have the following theorem.

Theorem 3.1.1. *Let $y^2 = 4x^3 + ax + b$ be an equation defining an elliptic curve E over $\mathbb{C}$ with real roots $e_1 < e_2 < e_3$. Then E can be realized as the* *period lattice generated by the periods*

$$\omega_1 = \int_{\infty}^{e_1} \frac{dw}{\sqrt{(w-e_1)(w-e_2)(w-e_3)}},$$
$$\omega_2 = \int_{\infty}^{e_2} \frac{dw}{\sqrt{(w-e_1)(w-e_2)(w-e_3)}},$$

where e_1, e_2, e_3 *are the roots of the equation defining* E*.*

Proof. We have

$$\begin{aligned}&\int_u^v \frac{dw}{\sqrt{(w-e_1)(w-e_2)(w-e_3)}}\\ &= \int_u^v \frac{dw}{\sqrt{4(\wp(\wp^{-1}(w))-e_1)(\wp(\wp^{-1}(w))-e_2)(\wp(\wp^{-1}(w))-e_3)}}\\ &= \int_u^v \frac{dw}{\wp'(\wp^{-1}(w))}\\ &= \wp^{-1}(u) - \wp^{-1}(v).\end{aligned}$$

Letting $v \to \infty$ and $u = \wp(z)$ gives

$$z = \frac{1}{2}\int_{\infty}^{\wp(z)} [(w-e_1)(w-e_2)(w-e_3)]^{-1/2} dw.$$

Substituting the half-periods $\omega_1, \omega_2, (\omega_1+\omega_2)/2$ for z then completes the proof.

□

In the next section we will give a method for evaluating the period integrals above. This method makes use of the j-invariant of an elliptic curve, which we will soon define.

3.2 The Inverse Problem

Here we introduce Klein's modular function j, also known as Klein's j-invariant, and explain how to use it in order to evaluate the period integrals described in the previous section. The j function is a modular function on $\mathrm{SL}_2(\mathbb{Z})$ and gives a bijection from the fundamental domain $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ to $\mathbb{C}$. We will discuss the problem of inverting the j function, which can be solved by the method used to evaluate the period integrals. In order to address the question of evaluating period integrals, we must define the arithmetic-geometric mean [2], a common limit of two recursively defined sequences discovered by Gauss.

Definition 3.2.1. Let $0 < b_0 < a_0$ and consider the recursively-defined sequences

$$a_{n+1} := \frac{a_n + b_n}{2}, \qquad b_{n+1} := \sqrt{a_n b_n}.$$

The common limit of a_n and b_n is called the **arithmetic-geometric mean** (AGM) and is denoted by $M(a_0, b_0)$.

The following theorem from [4] shows that when the roots of an Weierstrass cubic are all real, the period integrals described in the period integrals are given in terms of the arithmetic-geometric mean.

Theorem 3.2.2. *Suppose $e_1 < e_2 < e_3$. The period integrals are given up to sign in terms of the arithmetic-geometric mean by*

$$\omega_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}} = \frac{\pi}{M(\sqrt{e_3-e_1}, \sqrt{e_3-e_2})}$$

Proof. Making the change of variables $\sqrt{x-e_1} = \sqrt{e_2-e_1}\sin\theta$, we obtain

$$\omega_1 = 2\int_0^{\pi/2} \frac{d\theta}{\sqrt{(e_3-e_2)\sin^2\theta + (e_3-e_1)\cos^2\theta}}.$$

Making the change of variables $\sqrt{x-e_2} = \sqrt{e_1-e_2}\cos\theta$, we obtain

$$\omega_2 = 2i\int_0^{\pi/2} \frac{d\theta}{\sqrt{(e_2-e_1)\sin^2\theta + (e_3-e_1)\cos^2\theta}}.$$

The proposition will thus follow if we show that

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

is given by

$$I(a,b) = \frac{\pi}{2M(a,b)}$$

for $0 < a < b$. We will prove that

$$I(a,b) = I\left(\sqrt{ab}, \frac{a+b}{2}\right).$$

Passing to the limit gives

$$I(a,b) = I(M(a,b), M(a,b)).$$

The theorem will then follow as the integral on the right-hand side is easily seen to be $\pi/2M(a,b)$. The function

$$\frac{2at}{(b+a)+(b-a)t^2}$$

is increasing in t on $[0,1]$. We may thus make the change of variables

$$\sin\theta = \frac{2b\sin\varphi}{(b+a)+(b-a)\sin^2\varphi}, \qquad 0 \le \varphi \le \frac{\pi}{2}.$$

First we rewrite our integral as

$$I(a,b) = \int_0^{\pi/2} \frac{\cos\theta}{\cos^2\theta\sqrt{a^2\tan^2\theta + b^2}} d\theta.$$

We have

$$\cos\theta d\theta = \frac{2b\cos\varphi[(b+a)-(b-a)\sin^2\varphi]d\varphi}{[(b+a)+(b-a)\sin^2\varphi]^2}$$
$$\cos^2\theta = \frac{\cos^2\varphi[(b+a)^2-(b-a)^2\sin^2\varphi]}{[(b+a)+(b-a)\sin^2\varphi]^2}$$
$$\tan^2\theta = \frac{4b^2\sin^2\varphi}{\cos^2\varphi[(b+a)^2-(b-a)^2\sin^2\varphi]}.$$

Substituting and simplifying gives us

$$I(a,b) = \int_0^{\pi/2} \frac{2d\varphi}{\sqrt{4ab\sin^2\varphi+(b+a)^2\cos^2\varphi}},$$

which proves the theorem. □

We have reduced the problem of evaluating the period integrals to calculating the arithmetic-geometric mean. A discovery due to Gauss shows that the arithmetic-geometric mean can be evaluated in terms of the Gaussian hypergeometric series, which we define below.

Definition 3.2.3. The Gaussian hypergeometric series is defined for $|z| < 1$ by

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

where $(q)_n := q(q+1)\cdots(q+n-1)$ is the rising factorial.

Theorem Theorem 3.2.2 shows that the arithmetic-geometric mean is given in terms of the integrals

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

Rewriting $\cos^2\theta = 1-\sin^2\theta$ and simplifying, we find that

$$I(a,b) = \frac{1}{b}\int_0^{\pi/2} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}},$$

where $k = \sqrt{(b^2 - a^2)/b^2} < 1$. The integral above is called the **complete elliptic integral of the first kind** and is denoted by $K(k)$. The following theorem shows that $K(k)$ can be evaluated in terms of the hypergeometric series.

Theorem 3.2.4. *The complete elliptic integral of the first kind $K(k)$ has the series expansion*

$$K(k) = \frac{\pi}{2} \sum_{n=0}^{\infty} \left[\frac{(2n-1)!!}{(2n)!!} \right]^2 k^{2n} = \frac{\pi}{2} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; k^2\right).$$

Proof. We use the binomial theorem to rewrite the integrand as

$$\frac{1}{\sqrt{1 - k^2 \sin^2 \theta}} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-1)^n k^{2n} \sin^{2n} \theta.$$

Integrating term by term yields

$$\begin{aligned} K(k) &= \sum_{n=0}^{\infty} \binom{1/2}{n} (-1)^n k^{2n} \int_0^{\pi/2} \sin^{2n} \theta d\theta \\ &= \sum_{n=0}^{\infty} \binom{1/2}{n} (-1)^n k^{2n} \frac{1}{4^n} \binom{2n}{n} \frac{\pi}{2} \\ &= \frac{\pi}{2} \sum_{n=0}^{\infty} \frac{(-1/2)(-1/2-1)\cdots(-1/2-n+1)}{n!} (-1)^n k^{2n} \frac{1}{4^n} \frac{(2n)!}{(n!)^2} \\ &= \frac{\pi}{2} \sum_{n=0}^{\infty} \left[\frac{(2n-1)!!}{(2n)!!} \right]^2 k^{2n}. \end{aligned}$$

□

We summarize our results thus far about period integrals in the following theorem:

Theorem 3.2.5. *Let $y^2 = 4x^3 - g_2 x - g_3$ is a Weierstrass model for an elliptic curve $E(\mathbb{C})$ with real roots $e_1 < e_2 < e_3$. Then $E(\mathbb{C})$ is isomorphic to* *the complex torus $\mathbb{C}/\Lambda$, where Λ is the lattice generated by periods*

$$\omega_1 = \frac{\pi}{\sqrt{e_3-e_2}} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \frac{e_1-e_2}{e_3-e_2}\right), \qquad \omega_2 = \frac{\pi}{\sqrt{e_2-e_1}} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \frac{e_2-e_3}{e_2-e_1}\right).$$

Proof. By Theorem 3.2.2, we have

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

By Theorem 3.2.2 and 3.2.4, if $0 < a < b$ then we have

$$M(a,b) = \frac{\pi}{2I(a,b)} = \frac{b}{{}_2F_1(1/2, 1/2; 1; k^2)},$$

where $k = \sqrt{1-a^2/b^2}$. Setting $a = \sqrt{e_3-e_1}$ and $b = \sqrt{e_3-e_2}$ for ω_1 and $b = \sqrt{e_2-e_1}$ for ω_2, we have $k = \sqrt{(e_1-e_2)/(e_3-e_2)}$ for ω_1 and $k = \sqrt{(e_2-e_3)/(e_2-e_1)}$ for ω_2. Substituting yields the proposition. □

We use the above theorem to compute the period lattices of a few examples of elliptic curves.

Example 3.2.6. Consider the elliptic curve

$$y^2 = 4x^3 - 4x.$$

We factor the cubic to write

$$y^2 = 4x(x+1)(x-1),$$

thus $e_1 = -1, e_2 = 0, e_3 = 1$. Substituting the roots into the formula for k from theorem 3.2.5, we find that $k^2 = -1$ for ω_1 and ω_2. Then by theorem 3.2.5,

ω_1 and ω_2 are given by

$$\omega_1 = \pi {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; -1\right), \qquad \omega_2 = \pi i {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; -1\right).$$

Computing the above expression in Mathematica and truncating to 6 decimal places, we find that

$$\omega_1 = 2.622058\ldots, \qquad \omega_2 = 2.622058\ldots i,$$

thus the period lattice is square.

Example 3.2.7. Consider the elliptic curve

$$y^2 = 4x^3 - 16x^2 + 12x.$$

We factor the cubic to write

$$y^2 = 4x(x-1)(x-3),$$

thus $e_1 = 0, e_2 = 1, e_3 = 3$. Substituting the roots into the formula for k from theorem 3.2.5, we find that $k^2 = -1/2$ for ω_1 and $k^2 = -2$ for ω_2. Then by theorem 3.2.5, ω_1 and ω_2 are given by

$$\omega_1 = \frac{\pi}{\sqrt{2}} {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; -\frac{1}{2}\right), \qquad \omega_2 = \pi i {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; -2\right).$$

Computing the above expression in Mathematica and truncating to 6 decimal places, we find that

$$\omega_1 = 2.002155\ldots, \qquad \omega_2 = 2.342840\ldots i.$$

We now move on to discussion of the j-invariant. We make the following definition.

Definition 3.2.8. If ω_2/ω_1 is not real we define Klein's j-invariant by

$$j(\omega_1, \omega_2) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)},$$

where $\Delta(\omega_1, \omega_2) := g_2^3 - 27g_3^2$ is the **modular discriminant**. Since g_2^3 and Δ are both homogeneous of the same degree, we have $j(1, \tau) = j(\omega_1, \omega_2)$, where $\tau = \omega_2/\omega_1$. We may thus consider j as a function of one complex variable τ.

Given a Weierstrass cubic model $y^2 = 4x^3 - g_2x - g_3$ for an elliptic curve E, we say that

$$\frac{g_2^3}{g_2^3 - 27g_3^2}$$

is the j-invariant of E, denoted by $j(E)$. The following theorem shows that the term "invariant" is not misguided:

Theorem 3.2.9. *Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if they have the same j-invariant.*

Proof. Two elliptic curves over $\mathbb{C}$ are isomorphic if and only if there exists an isomorphism of the form $(x, y) \to (u^2z, u^3w)$ for some nonzero $u \in \mathbb{C}$. Consider an elliptic curve E defined by $y^2 = 4x^3 - ax - b$. The change of coordinates $(x, y) \to (u^2z, u^3w)$ produces an elliptic curve

$$w^2 = z^3 + a'z + b',$$

with $a' = u^{-4}a$ and $b' = u^{-6}b$. We find that

$$\frac{a^3}{a^3 - 27b^2} = \frac{(u^{-4}a)^3}{(u^{-4}a)^3 - 27(u^{-6}b)^2}.$$

Conversely, suppose we have two elliptic curves E_1 and E_2 with Weierstrass equations

$$y^2 = 4x^3 - ax - b, \qquad y^2 = 4x^3cx - d,$$

respectively such that $j(E_1) = j(E_2)$. Then

$$\frac{a^3}{a^3 - 27b^2} = \frac{c^3}{c^3 - 27d^2},$$

i.e.,

$$\frac{\frac{a^3}{b^2}}{\frac{a^3}{b^2} - 27} = \frac{\frac{c^3}{d^2}}{\frac{c^3}{d^2} - 27}.$$

We see that $\frac{a^3}{b^2} = \frac{c^3}{d^2}$. If a and b are nonzero, we may thus define an isomorphism by letting

$$u = (c/a)^{1/4} = (d/b)^{1/6}.$$

Now if $a = 0$, then $j(E_1) = j(E_2) = 0$, hence $c = 0$. An isomorphism is given by letting $u = (b/c)^{1/6}$. If $b = 0$ and $a \neq 0$, then an isomorphism is given by letting $u = (b/a)^{1/6}$. □

We now discuss the inverse problem. Given a complex number α, one wishes to produce $\tau \in \mathbb{H}$ such that $j(\tau) = \alpha$. The problem can be solved in following way. First, write down a Weierstrass model for an elliptic curve E with j-invariant equal to α. Using the method described in this section, one produces periods ω_1, ω_2 such that $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$, where Λ is the lattice generated by ω_1, ω_2. Then we may take $\tau = \omega_2/\omega_1$. The following proposition shows how to produce a Weierstrass equation for an elliptic curve with a given nonzero j-invariant. Since $j(\omega_1, \omega_2) = 0$ is equivalent to $g_2(\omega_1, \omega_2) = 0$, an elliptic curve has j-invariant equal to 0 if and only if it is of the form $y^2 = 4x^3 - g_3$ where $g_3 \neq 0$.

Proposition 3.2.10. *Let $\alpha \in \mathbb{C}$ be nonzero. A Weierstrass equation for an* *elliptic curve with j-invariant equal to α is*

$$y^2 = 4x^3 - g_2 x - g_3,$$

where

$$a = \frac{1}{27}\left(1 - \frac{1}{\alpha}\right)$$

and $g_3 = a^{1/2} g_2^{3/2}$ with g_2 an arbitrary nonzero complex number.

Proof. The j-invariant of our elliptic curve is given by

$$\frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{g_2^3}{g_2^3 - 27ag_2^3} = \frac{1}{1-27a} = \frac{1}{1-(1-\alpha^{-1})} = \alpha.$$

□

Aside from parametrizing isomorphism classes of elliptic curves, the j-invariant is interesting in its own right as a function of τ. The following proposition shows that j is invariant under $\mathrm{SL}_2(\mathbb{Z})$ transformations:

Proposition 3.2.11. *If a, b, c, d are integers with $ad - bc = 1$, then*

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau),$$

i.e., j is a modular function on $SL_2(\mathbb{Z})$.

Proof. Suppose ω_1, ω_2 are periods with ratio $\omega_2/\omega_1 = \tau \in \mathbb{H}$. Let $\omega_1' = c\omega_1 + d\omega_2$ and $\omega_2' = a\omega_1 + b\omega_2$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. The pairs $\{\omega_1', \omega_2'\}$ and $\{\omega_1, \omega_2\}$ generate the same lattice in $\mathbb{C}$ by Proposition 2.1.2. Since j is a function of g_2 and g_3, which depend only on the lattice, the proposition follows so long as $\tau' = \omega_2'/\omega_1' \in \mathbb{H}$. We have

$$\tau' = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d},$$

thus the imaginary part of τ' is equal to

$$\frac{(a\tau+b)(c\bar{\tau}+d)}{|c\tau+d|^2} = \frac{\mathrm{Im}(\tau)(ad-bc)}{|c\tau+d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}.$$

Therefore $\tau' \in \mathbb{H}$ if and only if $\tau \in \mathbb{H}$. □

The following theorem shows that j as a function of τ is analytic in $\mathbb{H}$.

Theorem 3.2.12. *The functions $g_2(\tau), g_3(\tau), \Delta(\tau)$, and $j(\tau)$ are analytic in $\mathbb{H}$.*

Proof. Since Δ has no zeros in $\mathbb{H}$, it suffices to show that g_2 and g_3 are analytic in $\mathbb{H}$. Recall that g_2 and g_3 are both of the form

$$\sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq 0}} \frac{1}{(m+n\tau)^\alpha}$$

with $\alpha > 2$. We will prove that the above series converges absolutely for any fixed $\tau = x+iy \in \mathbb{H}$ and uniformly in every strip S of the form

$$S = \{x+iy : |x| \leq X, y \geq Y > 0\}.$$

The theorem will then follow. To prove the latter statement, we will show that there exists a constant $M > 0$ such that

$$\frac{1}{|m+n\tau|^\alpha} \leq \frac{M}{|m+ni|^\alpha}$$

for all $\tau \in S$ and all $(m,n) \neq (0,0)$. The sum over the right-hand side converges by Lemma 2.1.6.

It suffices to show that

$$|m+n\tau|^2 > K|m+ni|^2.$$

or equivalently

$$(m + nx)^2 + (ny)^2 > K(m^2 + n^2).$$

for some $K > 0$. If $n = 0$, the above inequality holds so long as $0 < K < 1$. For $n \neq 0$, set $r = m/n$. Dividing both sides of the above inequality by $(m^2 + n^2)$ and then dividing through by n^2 gives

$$\frac{(r + x)^2 + y^2}{1 + r^2} > K.$$

We will show this holds for all r with

$$K = \frac{Y^2}{1 + (X + Y)^2} < 1$$

if $x \leq X$ and $y \geq Y$.

If $|r| \leq X + Y$ the inequality holds since $y \geq Y$ and $(r + x)^2 \geq 0$. If $|r| > X + Y$ then

$$\left|\frac{x}{r}\right| < \frac{|x|}{X + Y} \leq \frac{X}{X + Y} < 1.$$

Therefore

$$\left|1 + \frac{x}{r}\right| \geq 1 - \left|\frac{x}{r}\right| > 1 - \frac{X}{X + Y} = \frac{Y}{X + Y},$$

Multiplying through by r gives

$$|r + x| \geq \frac{rY}{X + Y}.$$

Squaring both sides and dividing through by $1 + r^2$, we see that

$$\frac{(r + x)^2 + y^2}{1 + r^2} > \frac{Y^2}{(X + Y)^2} \frac{r^2}{1 + r^2}. \tag{3.2.1}$$

Since $r^2/(1+r^2)$ is increasing in r^2, we let $r = A + r$ to conclude that

$$\frac{r^2}{1+r^2} \geq \frac{(A+Y)^2}{1+(A+Y)^2}$$

when $r^2 > (A+\delta)^2$. We may thus let $r = (X+Y)^2$ on the right hand side of Section 3.2 to see that

$$\frac{(r+x)^2+y^2}{1+r^2} > \frac{Y^2}{1+(X+Y)^2} = K.$$

□

The following theorem shows that $j(\tau)$ has a Fourier expansion:

Theorem 3.2.13. *If* $\tau \in \mathbb{H}$, $j(\tau)$ *has an absolutely convergent Fourier expansion*

$$j(\tau) = \sum_{n=-\infty}^{\infty} a(n) e^{2\pi i n \tau}.$$

Proof. Let $q = e^{2\pi i \tau}$. Since $\mathrm{Im}(\tau) > 0$, we have

$$|q| = e^{-2\pi i \,\mathrm{Im}(\tau)} < 1.$$

Thus the map $\tau \to q$ maps $\mathbb{H}$ into the punctured unit disc $0 < |q| < 1$. Let

$$f(q) = j(\tau), \qquad q = e^{2\pi i \tau}.$$

If $e^{2\pi i \tau} = e^{2\pi i \tau'}$, then $\tau' = \tau + m$ for some integer m. The map $\tau \to \tau + m$ is an $\mathrm{SL}_2(\mathbb{Z})$-linear transformation with matrix representation $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. Proposition 3.2.11 thus ensures that f is well-defined. Now f is analytic in the punctured unit disc since

$$f'(q) = \frac{d}{dq} j(\tau) = j'(\tau)\frac{d\tau}{dq} = j'(\tau)/\frac{dq}{d\tau} = \frac{j'(\tau)}{2\pi i e^{2\pi i\tau}}.$$

Therefore f has an absolutely convergent Laurent expansion

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

about $q = 0$. Replacing q by $e^{2\pi i\tau}$ gives

$$j(\tau) = \sum_{n=-\infty}^{\infty} a(n)e^{2\pi i n\tau},$$

completing the proof. □

We will be interested in the Fourier coefficients of $j(\tau)$. We will first determine the Fourier coefficients of $g_2(\tau)$ and $g_3(\tau)$. Note that the proof of Theorem 3.2.13 depended only on the fact that $j(\tau + 1) = j(\tau)$. The absolute convergence of the series defining $g_2(\tau)$ and $g_3(\tau)$, thus the same proof can be used to show that $g_2(\tau)$ and $g_3(\tau)$ have Fourier expansions. We begin by finding Fourier expansions for

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^4}, \qquad \text{and} \qquad \sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^6}$$

for a fixed n.

Lemma 3.2.14. *For $\tau \in \mathbb{H}$ and $n > 0$ we have the Fourier expansions*

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3}\sum_{t=1}^{\infty} t^3 e^{2\pi i t n\tau}$$

and

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^6} = -\frac{8\pi^6}{15} \sum_{t=1}^{\infty} t^5 e^{2\pi i t n \tau}.$$

Proof. We begin with the partial fraction expansion of cot:

$$\pi \cot(\pi\tau) = \frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \left(\frac{1}{\tau+m} - \frac{1}{m} \right).$$

Let $q = e^{2\pi i \tau}$. Then $0 < |x| < 1$.

$$\pi \cot(\pi\tau) = \pi \frac{\cos(\pi\tau)}{\sin(\pi\tau)} = \pi i \frac{q+1}{q-1} = -\pi i \left(\frac{q}{1-q} + \frac{1}{1-q} \right).$$

Using the series expansion of $1/(1-q)$ about $q = 0$ in the unit disc, we find that

$$\pi \cot(\pi\tau) = -\pi i \left(\sum_{t=1}^{\infty} q^t + \sum_{k=0}^{\infty} q^t \right) = -\pi i \left(1 + 2 \sum_{t=1}^{\infty} q^t \right).$$

Equation the two identities for $\pi \cot(\pi\tau)$, we find that

$$\frac{1}{\tau} + \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \left(\frac{1}{\tau+m} - \frac{1}{m} \right) = -\pi i \left(1 + 2 \sum_{t=1}^{\infty} e^{2\pi i t n \tau} \right)$$

for $\tau \in \mathbb{H}$. Differentiating five times, we find that

$$-\frac{1}{\tau^2} - \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \frac{1}{(\tau+m)^2} = -(2\pi i)^2 \sum_{t=1}^{\infty} t e^{2\pi i t n \tau}$$

$$-3! \sum_{m=-\infty}^{\infty} \frac{1}{(\tau+m)^4} = -(2\pi i)^4 \sum_{t=1}^{\infty} t^3 e^{2\pi i t n \tau}$$

$$-5! \sum_{m=-\infty}^{\infty} \frac{1}{(\tau+m)^6} = -(2\pi i)^6 \sum_{t=1}^{\infty} t^5 e^{2\pi i t n \tau}$$

Replacing τ by $n\tau$ completes the proof. □

Now we are ready to obtain the Fourier expansions of $g_2(\tau)$ and $g_3(\tau)$.

Theorem 3.2.15. *For $\tau \in \mathbb{H}$ we have the Fourier expansions*

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{k=1}^{\infty}\sigma_3(k)e^{2\pi ik\tau}\right)$$

and

$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty}\sigma_5(k)e^{2\pi ik\tau}\right).$$

Proof. We write

$$\begin{aligned}
g_2(\tau) &= 60 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4}\\
&= 60\left[\sum_{\substack{m\in\mathbb{Z}\\m\neq 0}}\frac{1}{m^4} + \sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\left(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4}\right)\right]\\
&= 60\left[2\zeta(4) + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\frac{1}{(m+n\tau)^4}\right]\\
&= 60\left[\frac{2\pi^4}{90} + \frac{16\pi^4}{3}\sum_{n=1}^{\infty}\sum_{t=1}^{\infty}t^3q^{nt}\right]
\end{aligned}$$

with $q = e^{2\pi i\tau}$. In the sum in the last line we collect terms for which $nt = k$ to find that

$$\sum_{n=1}^{\infty}\sum_{t=1}^{\infty}t^3q^{nt} = \sum_{c=1}^{\infty}\sum_{d|k}k^3q^k = \sum_{k=1}^{\infty}\sigma_3(k)q^k.$$

This completes the proof for $g_2(\tau)$. The proof for $g_3(\tau)$ is analogous. □

The last step we must complete before determining the Fourier coefficients of $j(\tau)$ is to obtain the Fourier expansion for $\Delta(\tau)$.

Theorem 3.2.16. *If $\tau \in \mathbb{H}$ we have the Fourier expansion*

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}.$$

The coefficients $\tau(n)$ are integers. In particular $\tau(1) = 1$ and $\tau(2) = -24$.

Proof. Let

$$x = e^{2\pi i\tau}, \qquad A = \sum_{n=1}^{\infty} \sigma_3(n)q^n, \qquad B = \sum_{n=1}^{\infty} \sigma_5(n)q^n.$$

Then

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = \frac{64\pi^{12}}{27}\left[(1+240A)^3 - (1-504B)^2)\right].$$

We expand the right-hand side as

$$\begin{aligned}(1+240A)^3 - (1-504B)^2) &= 3(240)A + 3(240)^2A^2 + (240)^3A^3 + 2(504)B^2 - 504^2B^2 \\ &= 12^2(5A+7B) + 12^3(100A^2 - 147B^2 + 8000A^3).\end{aligned}$$

Now A and B have integer coefficients and we see that

$$5A + 7B = \sum_{n=1}^{\infty}[5\sigma_3(n) + 7\sigma_5(n)]q^n$$

and

$$5d^3 + 7d^5 = d^3(5+7d^2)$$

is divisible by 3 and 4, thus 12^3 divides each coefficient of $(1+240)^3 - (1 - 504B)^2$. Therefore

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left(12^3\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}\right) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}$$

and each $\tau(n)$ is an integer. Since the Fourier expansions of A and B have zero constant term, the $n = 1$ term of $(1+240A)^3 - (1-504B)^2)$ comes from the $12^2(5A+7B)$ term. Thus

$$\tau(1) = 12^{-3}(12^2(5\sigma_3(1) + 7\sigma_5(1)) = 1.$$

Similarly

$$\begin{aligned}\tau(2) &= 12^{-3}(12^2(5\sigma_3(2)+7\sigma_5(1))+12^3(100\sigma_3(1)^2-147\sigma_5(1)^2))\\ &= 12^{-3}(12^2(276)+12^3(-47))\\ &= -24.\end{aligned}$$

□

The following theorem describes the Fourier expansion of $j(\tau)$.

Theorem 3.2.17. *If $\tau \in \mathbb{H}$ we have the Fourier expansion*

$$12^3 j(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n) e^{2\pi i n\tau},$$

where the $c(n)$ are integers.

Proof. We will write I to denote any power series in $q = e^{2\pi i\tau}$ with integer coefficients. We have

$$g_2^3(\tau) = \frac{64}{27}\pi^{12}(1+240q+I)^3 = \frac{64}{27}\pi^{12}(1+720q+I)$$

and

$$\Delta(\tau) = \frac{64}{27}\pi^{12}[12^3 q(1-24q+I)],$$

hence

$$j(\tau) = \frac{g_2^3(\tau)}{\Delta(\tau)} = \frac{1+720q+I}{12^3 q(1-24q+I)} = \frac{1}{12^3 q}(1+720q+I)(1+24q+I).$$

Therefore

$$12^3 j(\tau) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n) q^n,$$

where the $c(n)$ are integers. □

From henceforth we shall denote by $j(\tau)$ the normalized j-invariant $12^3 j(\tau)$ and let $q := e^{2\pi i\tau}$. The first few $c(n)$ are given in [1]. We have

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots .$$

We conclude this chapter with the following theorem, which we state without proof.

Theorem 3.2.18. *The function $j(\tau)$ is bijective from $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ to $\mathbb{C} \cup \{\infty\}$. Moreover,*

$$j(e^{2\pi i/3}) = 0, \qquad j(i) = 1728, \qquad j(i\infty) = \infty.$$

Chapter 4

Modular Forms and Harmonic Maass Forms

In this chapter we review the basics of modular forms and harmonic Maass forms.

4.1 Modular Forms

Here we define modular forms and review some of their basic properties given in [6]. Recall that a modular form is a meromorphic function on $\mathbb{H}$ which satisfies a transformation law with respect to groups of such transformations. We will be concerned with certain congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, which we now define.

Definition 4.1.1. If N is a positive integer, we define the level N **congruence**

subgroups as

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod N, \text{ and } c \equiv 0 \pmod N \right\}$$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod N, \text{ and } b \equiv c \equiv 0 \pmod N \right\}.$$

A congruence subgroup Γ acts on the **extended upper-half plane** $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ by fractional linear transformations as follows. Let $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. We let

$$\gamma\tau := \begin{cases} \frac{a\tau+b}{c\tau+d} & \text{if } \tau \neq \infty, \\ \frac{a}{c} & \text{if } \tau = \infty, \\ \infty & \text{if } \tau = -d/c. \end{cases}$$

.

Under this action, a Γ-orbit of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ is called a **cusp** of Γ. When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, there is a single cusp, which we denote by ∞. We will be interested in the stabilizer of ∞, which we denote by Γ_∞. The following proposition describes the elements of Γ_∞.

Proposition 4.1.2. *Let Γ_∞ denote the stabilizer of ∞. Then Γ_∞ is a subgroup* *of* $\Gamma_0(N)$ *for all* $N \geq 1$ *and*

$$\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}.$$

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\infty$. Then

$$M\infty = \frac{a\infty + b}{c\infty + d} = \infty.$$

If $c \neq 0$, then $M\infty = a/c$, thus we must have $c = 0$. This shows that $M \in \Gamma_0(N)$ for all $N \geq 1$. We then have $ac = 1$, thus $a = c = \pm 1$. We may assume $a = c = \pm 1$, as $M = -M$ are identified and both M and $-M$ are of the claimed form. □

Before we can define a modular form, we must first describe the following action of $\mathrm{GL}_2(\mathbb{R})$ on functions $f\colon \mathbb{H} \to \mathbb{C}$.

Definition 4.1.3. Suppose that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$. If $f\colon \mathbb{H} \to \mathbb{C}$ is a meromorphic function and k is an integer, we define the "slash" operator $|_k$ by

$$(f \mid_k \gamma)(\tau) := (\det \gamma)^{k/2}(cz + d)^{-k} f(\gamma\tau),$$

where

$$\gamma\tau := \frac{a\tau + b}{c\tau + d}.$$

We are now ready to give the definition of a modular form.

Definition 4.1.4. Suppose that $f\colon \mathbb{H} \to \mathbb{C}$ is a meromorphic function, that k is an integer, and that Γ is a congruence subgroup. Then f is called a

meromorphic modular form of integer weight k on Γ if f satisfies the following properties:

(i) We have
$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$$
for all $\tau \in \mathbb{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

(ii) If $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$, then $(f \mid_k \gamma_0)(\tau)$ has a Fourier expansion of the form
$$(f \mid_k \gamma_0)(\tau) = \sum_{n=n_{\gamma_0}}^{\infty} a_{\gamma_0}(n) q_N^n,$$
where $q_N := e^{2\pi i\tau/N}$ and $a_{\gamma_0}(n_{\gamma_0}) \neq 0$.

If $k = 0$, then f is known as a **modular function on** Γ.

Furthering the above definition, we say that f is **holomorphic modular (resp. cusp) form** if f is holomorphic on $\mathbb{H}$ and is holomorphic (resp. vanishes) at the cusps of Γ. We say that f is a weakly holomorphic modular form if its poles are supported at the cusps of Γ. We denote the complex vector space of modular forms (resp. cusp forms) by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$).

We conclude this section with a description of the fundamental domain for the modular group $\mathrm{SL}_2(\mathbb{Z})$. We make the following definition:

Definition 4.1.5. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. An open set R_Γ is called a **fundamental region of** Γ if it has the following two properties:

(a) $M\tau_1 \neq \tau_2$ for all $M \in \Gamma$ and all $\tau_1 \neq \tau_2$ in R_Γ.

(b) If $\tau \in \mathbb{H}$, then there is a point τ' in the closure of R_Γ such that $\tau = M\tau'$ for some $M \in \Gamma$.

As we have noted before, the j-invariant is a bijective function from any fundamental region for the whole modular group (with appropriate conditions on the boundary) to $\mathbb{C}$. We will thus be interested in determining a fundamental region for $\mathrm{SL}_2(\mathbb{Z})$. The set consisting of $\tau \in \mathbb{H}$ satisfying

$$|\tau| > 1, \qquad |\tau + \bar{\tau}| < 1$$

is a fundamental region for $\mathrm{SL}_2(\mathbb{Z})$. We will refer to this set, taken together with the points $\tau \in \mathbb{H}$ satisfying

$$|\tau| \geq 1, \qquad \mathrm{Re}(\tau) = -\frac{1}{2}$$

and those satisfying

$$|\tau| = 1, \qquad -\frac{1}{2} < \mathrm{Re}(\tau) \leq 0$$

as the **fundamental domain** for $\mathrm{SL}_2(\mathbb{Z})$, donated by $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. We will prove that this set is indeed a fundamental region for the modular group, but first we will need a few preliminaries, the first of which provides a generating set for the modular group.

Theorem 4.1.6. *The modular group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the two matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \textit{and} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We may assume that $c \geq 0$ since if not, we may multiply by $-I$ to obtain an equivalent matrix with $c \geq 0$. We will induct on c. If $c = 0$, then $a = d = \pm 1$. Multiply M by $-I$ if necessary so that $c = d = 1$. Then we have

$$M = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b.$$

If $c = 1$ then $ad - b = 1$, i.e., $b = ad - 1$ and we have

$$M = \begin{pmatrix} a & ad-1 \\ 1 & d \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} = T^a S T^d.$$

Now assume the theorem is true for all M with $c < C$. Let $M \in \mathrm{SL}_2(\mathbb{Z})$ with $c \leq C$. Since $ad - bc = 1$ we have $\gcd(c, d) = 1$, thus we may write

$$d = cq + r, \qquad 0 < r < c.$$

Then

$$AT^{-q} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix}$$

and

$$AT^{-q}S = \begin{pmatrix} a & -aq+b \\ c & r \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -aq+b & -a \\ r & -c \end{pmatrix}.$$

Since $r < C$, the matrix on the right-hand side above is generated by S and T, thus so is A, completing the induction step. □

Next we need the following lemma concerning fundamental pairs of periods.

Lemma 4.1.7. *Let $\omega_1', \omega_2' \in \mathbb{C}$ with ω_2'/ω_1' not real. Let*

$$\Omega = \{m\omega_1' + n\omega_2' : m, n \in \mathbb{Z}\}.$$

Then there exist a fundamental pair (ω_1, ω_2) *equivalent to* (ω_1', ω_2') *such that*

$$|\omega_2| \geq |\omega_1|, \qquad |\omega_1 + \omega_2| \geq |\omega_2|, \qquad |\omega_1 - \omega_2| \geq |\omega_2|.$$

Proof. Arrange the elements of Ω in a sequence

$$\Omega = \{0, w_1, w_2, \ldots\}$$

such that

$$0 < |w_1| \leq |w_2| \leq \cdots \quad \text{and} \quad \arg w_n < \arg w_{n+1} \quad \text{if} \quad |w_n| = |w_{n+1}|.$$

Let $\omega_1 = w_1$ and let ω_2 be the first element of this sequence such that $\arg \omega_2 \neq \arg \omega_1$. Since the sequence is ordered by increasing absolute value, the interior of the triangle with vertices $0, \omega_1, \omega_2$ contains no elements of Ω. Therefore (ω_1, ω_2) is a fundamental pair by Chapter 3. Since $\omega_1 \pm \omega_2$ are elements of Ω sequenced after ω_1 and ω_2, we have

$$|\omega_2| \geq \omega_1 \qquad \text{and } |\omega_1 \pm \omega_2|.$$

□

With the above lemma in hand, we can prove that the fundamental domain contains a full set of equivalent points of $\mathbb{H}$. This is the content of the following proposition.

Proposition 4.1.8. *If* $\tau' \in \mathbb{H}$*, there exists some* $\tau \in \mathbb{H}$ *equivalent to* τ' *under* $\mathrm{SL}_2(\mathbb{Z})$ *such that*

$$|\tau| \geq 1, \qquad |\tau + \bar{\tau}| \leq 1.$$

Proof. Let $\omega_1' = 1$ and $\omega_2' = \tau'$ and apply Lemma 4.1.7 to obtain a fundamental pair (ω_1, ω_2) with

$$|\omega_2| \geq |\omega_1|, \qquad |\omega_1 \pm \omega_2| \geq |\omega_2|.$$

By Proposition 2.1.2 there exists some $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix},$$

thus

$$\tau' = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1}.$$

Dividing the numerator and denominator by ω_1 and setting $\tau = \omega_2/\omega_1$, we see that $\tau = M\tau'$. Dividing the inequalities through by ω_1 gives

$$|\tau| \geq 1, \qquad |\tau \pm 1| \geq |\tau|.$$

To complete the proof, observe that $|\tau \pm 1| \geq |\tau|$ is equivalent to

$$2|\operatorname{Re}(\tau)| = |\tau + \bar{\tau}| \leq 1.$$

□

We are now ready to prove that

$$R = \{\tau \in \mathbb{H} : |\tau| > 1, |\tau + \bar{\tau}| < 1\}$$

is a fundamental region for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 4.1.9. *The open set*

$$R = \{\tau \in \mathbb{H} : |\tau| > 1, |\tau + \bar{\tau}| < 1\}$$

is a fundamental region for $\mathrm{SL}_2(\mathbb{Z})$*. Moreover, if* $M \in \mathrm{SL}_2(\mathbb{Z})$ *has a fixed point, then* $M = I$*.*

Proof. Proposition 4.1.8 shows that every point $\tau \in \mathbb{H}$ has some $SL_2(\mathbb{Z})$ equivalent in R. We need to show that no two distinct points in R are equivalent. Suppose $\tau' = M\tau$, where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. First we claim that $\mathrm{Im}(\tau') < \mathrm{Im}(\tau)$ if $\tau \in R$ and $c \neq 0$. We have

$$\mathrm{Im}(\tau') = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}.$$

If $\tau \in R$ and $c \neq 0$, we have

$$|c\tau + d|^2 = (c\tau + d)(c\bar{\tau} + d) = c^2\tau\bar{\tau} + cd(\tau + \bar{\tau}) + d^2 > c^2 - |cd| + d^2.$$

If $d = 0$ we see that

$$|c\tau + d|^2 > c^2 \geq 1.$$

If $d \neq 0$ we have

$$c^2 - |cd| + d^2 = (|c| - |d|)^2 + |cd| \geq |cd| \geq 1,$$

so again $|c\tau + d|^2 \geq 1$. Thus $c \neq 0$ implies $|c\tau + d|^2 > 1$. This proves the claim.

Now suppose $\tau, \tau' \in R$. Then

$$\tau' = \frac{a\tau + b}{c\tau + d}, \qquad \text{and} \qquad \frac{d\tau' - b}{-c\tau' + a}.$$

If $c \neq 0$ we have $\mathrm{Im}(\tau') < \mathrm{Im}(\tau)$ $\mathrm{Im}(\tau') > \mathrm{Im}(\tau)$, so we must have $c = 0$.

Therefore $ad = 1$, hence $a = d = \pm 1$. We thus have

$$M = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = T^{\pm b}.$$

Therefore $\tau' = \tau + b$. But $\tau, \tau' \in R$, thus

$$|b| = |\operatorname{Re}(\tau' - \tau)| < 1,$$

implying that $b = 0$. This shows that $\tau = \tau'$.

To prove the second part, simply follow the same argument and conclude again that $M = I$. □

In the following section we discuss the modular forms we will use to study the inverse problem.

4.2 Monstrous Forms

Here we discuss the forms we will be studying in our investigation of the inverse problem, which we will refer to as **monstrous forms**. Suppose $\alpha \in \mathbb{C}$ and $j(z) = \alpha$, where $z \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Let

$$H_z(\tau) := -\frac{1}{2\pi i}\frac{j'(\tau)}{j(\tau) - j(z)} = \sum_{n=0}^{\infty} j_n(z) q^n.$$

We shall refer to $H_z(\tau)$ as a monstrous form. Now $H_z(\tau)$ is a weight 2 meromorphic modular form and has a single simple pole at z. In Chapter 4 we explore the problem of numerically computing z by studying the asymptotics of the Fourier coefficients $j_n(z)$.

4.3 Harmonic Maass Forms

Here we define harmonic Maass forms. Throughout this section we let $\tau = u + iv \in \mathbb{H}$. We also let $\left(\frac{c}{d}\right)$ denote the extended Legendre symbol and define

$$\varepsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv 3 \pmod 4 \end{cases}$$

.

for odd integers d. In order to define harmonic Maass forms we must first define the weight k hyperbolic Laplacian operator.

Definition 4.3.1. For $k \in \mathbb{R}$, the **weight k hyperbolic Laplacian operator** on $\mathbb{H}$ is defined by

$$\Delta_k := -v^2\left(\frac{\partial^2}{\partial u^2} + \frac{\partial^2}{\partial v^2}\right) + ikv\left(\frac{\partial}{\partial u} + i\frac{\partial}{\partial v}\right) = -4v^2\frac{\partial}{\partial \tau}\frac{\partial}{\partial \tau} + 2ikv\frac{\partial}{\partial \bar{\tau}}.$$

Weight k harmonic Maass forms are real-analytic functions on $\mathbb{H}$ which are annihilated by Δ_k and which satisfy certain

Definition 4.3.2. If $k \in \frac{1}{2}\mathbb{Z}$ and Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with $\Gamma \subseteq \Gamma_0(4)$ if $k \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$, then a **weight k harmonic Maass form on Γ** is a smooth function satisfying the following properties:

(i) For all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and all $\tau \in \mathbb{H}$, we have

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = \begin{cases} (c\tau + d)^k f(\tau) & \text{if } k \in \mathbb{Z}, \\ \left(\frac{c}{d}\right)^{2k} \varepsilon_d^{-2k}(c\tau + d)^k f(\tau) & \text{if } k \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}. \end{cases}$$

.

(ii) We have that $\Delta_k(f) = 0$.

(iii) There exists a polynomial $P_f(\tau) \in \mathbb{C}[q^{-1}]$ such that

$$f(\tau) - P_f(\tau) = O\left(e^{-\epsilon v}\right)$$

as $v \to \infty$ for some $\epsilon > 0$. Analogous conditions are required at all cusps.

We denote by $H_k(\Gamma)$ the space of weight k harmonic Maass forms.

4.4 Divisors of Modular Forms

Here we discuss the recent work of Bringmann et al. [5] which will be using in order to investigate the inverse problem. The authors construct forms $H_z(\tau)$ which generalize the monstrous forms. If $f(\tau)$ is a weight k meromorphic modular form on $\mathrm{SL}_2(\mathbb{Z})$, then the **divisor modular form** is

$$f^{\mathrm{div}}(\tau) := \sum_{z \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}} e_z \operatorname{ord}_z(f) H_z(\tau).$$

In [3] it was shown that

$$f^{\mathrm{div}}(\tau) = -\frac{\Theta(f(\tau))}{f(\tau)} + \frac{kE_2(\tau)}{12}, \tag{4.4.1}$$

where $\Theta := \frac{1}{2\pi i}\frac{d}{d\tau}$. In [5] the authors generalize these results for meromorphic modular forms on $\Gamma_0(N)$. They construct weight 2 harmonic Maass forms $H^*_{N,z}(\tau)$ which generalize the $H_z(\tau)$ and define the **divisor polar harmonic Maass form**

$$f^{\mathrm{div}}(\tau) := \sum_{z \in \Gamma_0(N) \backslash \mathbb{H}} e_{N,z} \operatorname{ord}_z(f) H^*_{N,z}(\tau),$$

where $e_{N,z} := 2/\#\operatorname{Stab}_z(\Gamma_0(N))$. Generalizing Equation (4.4.1), they show that

$$f^{\mathrm{div}}(\tau) \equiv \frac{k}{4\pi \operatorname{Im}(\tau)} - \frac{\Theta(f(\tau))}{f(\tau)} \pmod{S_2(\Gamma_0(N))}.$$

When $N = 1$, we have that $H_{1,z}(\tau) = H_z(\tau) - E_2^*(\tau)$, where $E_2^*(\tau) := -\frac{3}{\pi \operatorname{Im}(\tau)} + E_2(\tau)$ is the usual weight 2 nonholomorphic Eisenstein series, and $j_{1,n}(\tau) = j_n(\tau)$. We now quote Theorem 1.1 of [5], which summarizes the facts about the $H_{N,z}^*(\tau)$ we have explained thus far. Crucially, it also describes the growth of the coefficients $j_{N,n}(\tau)$ in n-aspect. These asymptotics are given in terms of "Ramanujan-like" expansions, sums of the form

$$\sum_{\lambda \in \Lambda_z} \sum_{(c,d) \in S_\lambda} \frac{1}{\lambda^k} e\left(-\frac{n}{\lambda} r_z(c,d,k)\right) e^{\frac{2\pi n \operatorname{Im}(z)}{\lambda}},$$

for some real numbers $r_z(c,d,k)$, Λ_z a lattice in $\mathbb{R}$, and S_λ the set of solutions to $Q_z(c,d) = \lambda$ for a certain positive-definite binary quadratic form Q_z.

Theorem 4.4.1. *If $z \in \mathbb{H}$, then $H_{N,z}^*(\tau)$ is a weight 2 polar harmonic Maass form on $\Gamma_0(N)$ which vanishes at all cusps and has a single simple pole at z. Moreover, the following are true:*

(1) If $z \in \mathbb{H}$ and $\operatorname{Im}(\tau) > \max\{\operatorname{Im}(z), \frac{1}{\operatorname{Im}(z)}\}$, then we have that

$$H_{N,z}^*(\tau) = \frac{3}{\pi[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] \operatorname{Im}(\tau)} + \sum_{n=1}^{\infty} j_{N,n}(z) q^n.$$

(2) For $(N,n) = 1$, we have $j_{N,n}(\tau) = j_{N,1}(\tau) \mid T(n)$.

(3) For $n \mid N$, we have $j_{N,n}(\tau) = j_{\frac{N}{n},1}(n\tau)$.

(4) As $n \to \infty$, we have

$$j_{N,n}(\tau) = \sum_{\substack{\lambda \in \Lambda_\tau \\ \lambda \leq n}} \sum_{(c,d) \in S_\lambda} e\left(-\frac{n}{\lambda} r_\tau(c,d)\right) e^{\frac{2\pi n \operatorname{Im}(\tau)}{\lambda}} + O_\tau(n).$$

An analogous theorem is proven for z a cusp of $\Gamma_0(N)$.

In Chapter 3.2 we explained how the inverse problem can be approached by studying the asymptotics of the Fourier coefficients of the monstrous forms. This method is based on the following corollary to the Theorems 1.1-1.3 of [5]

Corollary 4.4.2. *Suppose that $f(\tau)$ is a meromorphic modular form of weight k on $\Gamma_0(N)$ whose divisor is not supported at cusps. Let y_1 be the largest imaginary part of any points in the divisor of $f(\tau)$ lying in $\mathbb{H}$. Then if $-\frac{\Theta(f(\tau))}{f(\tau)} =: \sum_{n \gg -\infty} a(n) q^n$, we have that*

$$y_1 = \limsup_{n \to \infty} \frac{\log |a(n)|}{2\pi n}.$$

The monstrous forms $H_z(\tau)$ have a single simple pole at z. Therefore Corollary 4.4.2 allows for numerical computation of $\operatorname{Im}(z)$. Once $\operatorname{Im}(z)$ is computed, Theorem 4.4.1 (4) can be used to numerically compute $\operatorname{Re}(z)$. In the following chapter, we prove Theorem 1.0.4.

Chapter 5

Proof of Theorem 1.0.4

In this chapter we prove Theorem 1.0.4. We begin by defining $r_z(c,d), \Lambda_z, S_\lambda$, and $Q_z(c,d)$. These objects appear in the sum

$$\sum_{\substack{\lambda\in\Lambda_z \\ \lambda\leq n}} \sum_{(c,d)\in S_\lambda} e\left(-\frac{n}{\lambda} r_z(c,d)\right) e^{\frac{2\pi n\,\mathrm{Im}(z)}{\lambda}}, \tag{5.0.1}$$

which gives an asymptotic formula for the coefficients $j_{N,n}(z)$ of the polar harmoinc Maass forms $H^*_{N,z}(\tau)$.

For an arbitrary solution $a, b \in \mathbb{Z}$ to $ad - bc = 1$, we define

$$\begin{aligned} r_z(c,d) &:= ac|z|^2 + (ad+bc)\,\mathrm{Re}(z) + bd, \\ \Lambda_z &:= \{\alpha|z|^2 + \beta\,\mathrm{Re}(z) + \gamma^2 : \alpha,\beta,\gamma \in \mathbb{Z}\}, \\ S_\lambda &:= \{(c,d) \in \mathbb{N}_0 \times \mathbb{Z} : \gcd(c,d) = 1 \text{ and } Q_z(c,d) = \lambda\}, \\ Q_z(c,d) &:= c^2|z|^2 + 2cd\,\mathrm{Re}(z) + d^2. \end{aligned}$$

Note that $r_z(c,d)$ is not uniquely defined. However, we claim that $e(-nr_z(c,d)/Q_z(c,d))$ is well defined. If

$$ad - bc = a'b - b'c = 1,$$

then $a' = a + mc$ and $b' = b + md$ for some $m \in \mathbb{Z}$. One easily checks that

$$r_z(a', b', c, d) - r_z(a, b, c, d) = mQ_z(c, d),$$

thus

$$\frac{nr_z(a', b', c, d)}{Q_z(c, d)} - \frac{nr_z(a, b, c, d)}{Q_z(c, d)} = nm.$$

This verifies the claim.

Our first task will be to simplify Equation (5.0.1) as $n \to \infty$ in the case $N = 1$, the case relevant to the proof of Theorem 1.0.4. We will show that Equation (5.0.1) can be rewritten as a sum over $\Gamma_\infty \backslash \Gamma_0(N)$. This form will be more convenient for obtaining our simplification.

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. We have

$$\operatorname{Re}(Mz) = \operatorname{Re}\left(\frac{az + b}{cz + d}\right) = \frac{ac|z|^2 + (ad + bc)\operatorname{Re}(z) + bd}{|cz + d|^2} = \frac{r_z(c, d)}{Q_z(c, d)}$$

and

$$\operatorname{Im}(Mz) = \operatorname{Im}\left(\frac{az + b}{cz + d}\right) = \frac{(ad - bc)\operatorname{Im}(z)}{|cz + d|^2} = \frac{\operatorname{Im}(z)}{Q_z(c, d)}.$$

The terms appearing in the sum in Equation (5.0.1) are equal to

$$e\left(-\frac{n}{\lambda} r_z(c, d)\right) e^{\frac{2\pi n \operatorname{Im}(z)}{\lambda}} = e^{-2\pi i n \frac{r_z(c,d)}{Q_z(c,d)}} e^{2\pi n \frac{\operatorname{Im}(z)}{Q_z(c,d)}} = e^{-2\pi i n \frac{r_z(c,d) + i \operatorname{Im}(z)}{Q_z(c,d)}}$$

for some $c, d \in N\mathbb{N}_0 \times \mathbb{Z}$ with $\gcd(c, d) = 1$, hence each term is equal to $e^{-2\pi i n M z}$ for some $M \in \Gamma_0(N)$. The following lemma gives the desired alternate form of Equation (5.0.1).

Lemma 5.0.3. *We have*

$$j_{N,n}(z) = \sum_{\substack{M \in \Gamma_\infty \backslash \Gamma_0(N) \\ n \operatorname{Im}(Mz) \geq \operatorname{Im}(z)}} e^{-2\pi i n M z} + O_z(n).$$

Proof. The restriction $n \operatorname{Im}(Mz) \geq \operatorname{Im}(z)$ is equivalent to the restriction $\lambda \leq n$. We only need show that if

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, M' = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

then M and M' are equivalent in $\Gamma_\infty \backslash \Gamma_0(N)$. We have

$$ad - bc = a'd - b'c = 1,$$

thus $a' = a + mc$ and $b' = b + md$ for some $m \in \mathbb{Z}$. Therefore

$$M' = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} M,$$

hence M and M' are equivalent in $\Gamma_\infty \backslash \Gamma_0(N)$. □

When $\operatorname{Im}(z) \geq \operatorname{Im}(Mz)$ for all $M \in \Gamma_0(N)$, the terms with $\operatorname{Im}(Mz) = \operatorname{Im}(z)$ in the sum appearing in the above lemma dominate. We explain this in more detail in the following proposition.

Proposition 5.0.4. *Let $z = x + iy$. If $y \geq \operatorname{Im}(Mz)$ for all $M \in \Gamma_0(N)$, then*

$$j_{N,n}(z) e^{-2\pi n y} \sim e^{-2\pi i n x} + \sum_{\substack{c \geq 1 \\ N | c}} \sum_{\substack{d \in \mathbb{Z} \\ \gcd(c,d)=1 \\ |cz+d|^2=1}} e^{-2\pi i n r_z(c,d)}.$$

Proof. We have

$$j_{N,n}(z) = \sum_{\substack{M \in \Gamma_\infty \backslash \Gamma_0(N) \\ n\,\mathrm{Im}(Mz) \geq \mathrm{Im}(z)}} e^{-2\pi i n M z} + O_z(n).$$

The hypothesis implies that the dominant terms are those for which $\mathrm{Im}(Mz) = y$. This holds if and only if $|cz+d|^2 = 1$. We isolate the term $e^{-2\pi i n z}$ arising from the unique $c = 0$ term, i.e., $M = I$, and rewrite $Mz = r_z(c,d) - y$ to obtain

$$j_{N,n}(z) = e^{-2\pi i n z} + \sum_{\substack{c \geq 1 \\ N|c}} \sum_{\substack{d \in \mathbb{Z} \\ \gcd(c,d)=1 \\ |cz+d|^2=1}} e(n r_z(c,d)) e^{2\pi n y} + O(n) + \varepsilon_z(n),$$

where $\varepsilon_z(n) = o(e^{2\pi n y})$. Dividing through by $e^{2\pi n y}$ and letting $n \to \infty$ proves the lemma. □

For the proof of Theorem 1.0.4, we will be interested in the case $N = 1$, i.e., $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. The following lemma shows that the condition $\mathrm{Im}(z) \geq \mathrm{Im}(Mz)$ holds for $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 5.0.5. *If $z \in SL_2(\mathbb{Z}) \backslash \mathbb{H}$, then*

$$\mathrm{Im}(z) \geq \mathrm{Im}(Mz)$$

for all $M \in SL_2(\mathbb{Z})$.

Proof. Let $z \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$. We must show that

$$|cz+d|^2 \geq 1$$

for all $c, d \in \mathbb{Z}$ with $\gcd(c,d) = 1$. Write $z = x + iy$. Since $z \in \mathrm{SL}_2(\mathbb{Z})$, we have $|z| \geq 1$, $|x| \leq \frac{1}{2}$, and $y \geq \frac{\sqrt{3}}{2}$. Now since $|z| \geq 1$ we may assume that $d \neq 0$. Clearly $|cz+d|^2 \geq 1$ holds if $c = 0$, so assume also that $c \neq 0$. We thus have

$$|\operatorname{Im}(cz+d)| = |cy| \geq y \geq \frac{\sqrt{3}}{2}$$

and

$$|\operatorname{Re}(cz+d)| = |cx+d| \geq ||cx| - |d|| \geq ||x| - |d|| \geq \frac{1}{2}.$$

This completes the proof. □

The following proposition is a specialization of Proposition 5.0.4 for the case $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. We will use it in order to calculate $\operatorname{Re}(z)$.

Proposition 5.0.6. *Let $z \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Write $z = x + iy$. We have*

(1) We have

$$j_n(z)e^{-2\pi ny} \sim e^{-2\pi inx} \qquad \text{if } |z| > 1,$$

(2) We have

$$j_n(z)e^{-2\pi ny} \sim 2\cos(2\pi nx) \qquad \text{if } |z| = 1, x > -\frac{1}{2}$$

(3) We have

$$j_n(z)e^{-2\pi ny} \sim e^{-2\pi ix} + 2e^{2\pi ix} \qquad \text{if } z = e^{2\pi i/3}.$$

Proof. Since $z \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, by Lemma 5.0.5, the asymptotic formula given in Proposition 5.0.4 holds. We have $y \geq \frac{\sqrt{3}}{2}$. From this we see that if $c \geq 2$, then $|cz+d| > 1$. The formula in Proposition 5.0.4 thus reduces to

$$j_{N,n}(z)e^{-2\pi ny} \sim e^{-2\pi inx} + \sum_{\substack{d\in\mathbb{Z} \\ |z+d|^2=1}} e^{-2\pi inr_z(1,d)}. \tag{5.0.2}$$

We have $|x| \leq \frac{1}{2}$, thus $|\operatorname{Re}(z+d)| \geq \frac{1}{2}$. Then since $|z| \geq 1$, we also have $|z+d| \geq 1$, with equality if and only if $|z| = 1$.

If $|z| > 1$, the sum appearing in Equation (5.0.2) is empty, proving (1).

If $|z| = 1$ but $x > -\frac{1}{2}$, then the $d = 0$ term appears, but the strict inequality $|z+d| > 1$ holds for all $d \neq 0$. Choosing $a = 0, b = -1$ gives $r_z(1,0) = -x$, proving (2).

If $z = e^{2\pi i/3}$, then $|z| = 1$ and $x = -\frac{1}{2}$. Then $z + 1 = e^{2\pi i/6}$, thus the $d = 1$ term appears. However, $|z+d| > 1$ still holds for all $d \neq 0, 1$. Choosing $a = 0, b = -1$ with $(c,d) = (1,1)$ gives $r_z(1,1) = -x-1$, proving (3). □

We are now ready to begin the proof of Theorem 1.0.4. We begin with the following proposition, which shows given $\alpha \in \mathbb{C}$ how to calculate the imaginary part of the $z \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $j(z) = \alpha$. Throughout the proof we let $z = x + iy$

Proposition 5.0.7. *Let $\alpha \in \mathbb{C}$ and let $z \in \mathrm{SL}_2(\mathbb{Z})$ such that $j(z) = \alpha$. Then*

$$y = \limsup_{n\to\infty} \frac{\log|a(n)|}{2\pi n}.$$

Proof. Recall that the monstrous form $H_z(\tau)$ has a single simple pole at z. We will identify y using the fact that Fourier expansion $H_z(\tau) = \sum_{n=0}^{\infty} a(n)q^n$ converges so long as $\operatorname{Im}(\tau) > y$. Let

$$y_1 = \limsup_{n\to\infty} \frac{\log|a(n)|}{2\pi n}.$$

Suppose $\tau - y_1 = d > 0$. Then for n sufficiently large we have

$$|a(n)e^{2\pi i n\tau}| = |a(n)|e^{-2\pi n(y_1+d)} \leq e^{-2\pi n d},$$

thus $\sum_{n=0}^{\infty} a(n)e^{2\pi n\tau}$ converges by comparison with $\sum_{n=0}^{\infty} e^{-2\pi n d}$ if $\tau > y_1$.

On the other hand, if $\tau = y_1$, then

$$\limsup_{n\to\infty} |a(n)e^{2\pi i n\tau}| = \limsup_{n\to\infty} |a(n)|e^{-2\pi n y_1} = 1,$$

thus $\sum_{n=0}^{\infty} a(n)e^{2\pi i n\tau}$ diverges if $\tau = y_1$. We conclude $y = y_1$. □

We will now show how to calculate x once y has been calculated to a sufficient level of precision. Let $H_z(\tau) = \sum_{n=0}^{\infty} a(n)q^n$ and let $c(n) = a(n)e^{-2\pi n y}$. By Proposition 5.0.6 we have

$$\cos(2\pi n x) \sim \frac{1}{2}c(n)$$

if $|z| = 1$ and

$$e^{-2\pi i n x} \sim c(n)$$

if $|z| > 1$.

We first address the question of determining whether $|z| = 1$ or $|z| > 1$. Note that

$$e^{-2\pi i n x} \sim c(n)$$

implies that

$$\lim_{n\to\infty} |c(n)| = 1,$$

thus if $|c(n)|$ is not converging to 1, then we must have $|z| = 1$. We claim that the converse is also true. If $|z| = 1$, then we have

$$\cos(2\pi n x) \sim \frac{1}{2}c(n).$$

If in addition we have

$$\lim_{n\to\infty} |c(n)| = 1,$$

then we have

$$\lim_{n\to\infty} |\cos(2\pi nx)| = \frac{1}{2}.$$

This is a contradiction, thus proving the claim.

By Proposition 5.0.7, we have

$$y = \limsup_{n\to\infty} \frac{\log|a(n)|}{2\pi n},$$

thus $c(n)$ is bounded by a constant for sufficiently large n. Thus Proposition 5.0.6 in fact guarantees that

$$\lim_{n\to\infty} \cos(2\pi nx) = \frac{1}{2}c(n)$$

if $|z| = 1$ and

$$\lim_{n\to\infty} \cos(2\pi nx) = \operatorname{Re}(c(n))$$

if $|z| > 1$. We thus need only give the proof for the case $|z| > 1$.

Let $w_n = \cos^{-1}(c(n))$. Then when n is sufficiently large, we have

$$c(n) \approx \cos(w_{n-1} \pm 2\pi x).$$

Now $|x| \leq \frac{1}{2}$ and $w_n \in [0, \pi]$, thus

$$-\pi \leq w_n \pm 2\pi x \leq 2\pi.$$

If $x_0 \in [-\pi, \pi]$, then $\cos^{-1}(\cos(x_0))$ is equal to $\pm x_0$, where the sign of x is positive if $x_0 \in [0, \pi]$ and negative if $x_0 \in [-\pi, 0)$. If $x_0 \in (\pi, 2\pi]$, then $\cos^{-1}(\cos(x_0))$ is equal to $2\pi - x_0$. We thus have

$$\pm w_n \approx w_{n-1} \pm 2\pi x$$

or

$$w_n \approx 2\pi - (w_{n-1} \pm 2\pi x)$$

Therefore

$$x \approx \pm\frac{1}{2\pi}(w_n \pm w_{n-1})$$

or

$$x \approx \pm\frac{1}{2\pi}(w_n + w_{n-1} - 2\pi).$$

The correct value can then be determined by substituting back into the asymptotic formula.

Chapter 6

Examples

In this chapter we provide some examples of calculating $z \in \mathrm{SL}_2(\mathbb{Z})$ such that $j(z) = \alpha$ for given values of α. Throughout this section we let $z = x + iy$ and we let

$$-\frac{\Theta(j(\tau))}{j(\tau) - \alpha} = \sum_{n=0}^{\infty} a(n) q^n,$$
$$b(n) = \frac{\log |a(n)|}{2\pi n},$$
$$c(n) = a(n) e^{-2\pi n y_1},$$

where y_1 is the approximation of y obtained by observing the convergence of the sequence $\{b(n)\}_{n=1}^{\infty}$.

Example 6.0.8. ($\alpha = 0$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)} = 1 - 744q + 159768q^2 + 36866976q^3 + 8507424792q^4 + \cdots .$$

We find that $b(1000) = 0.8662\ldots$ and see that $b(n) \to \frac{\sqrt{3}}{2}$. Letting $y_1 = \frac{\sqrt{3}}{2}$ we compute

$$c(999) = -3.000000\ldots,$$
$$c(1000) = 3.000000\ldots.$$

We see that $c(n) \approx (-1)^n \cdot 3$. Neither $e^{-2\pi i n x}$ nor $2\cos(2\pi n x)$ can exhibit such behavior, thus

$$c(n) \sim e^{-2\pi inx} + 2e^{2\pi inx}.$$

We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{3}i}{2}$.

Example 6.0.9. ($\alpha = 1728$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau) - 1728} = 1 - 984q + 574488q^2 + 307081056q^3 + 164453203992q^4 + \cdots .$$

We find that $b(1000) = 1.0001103178\ldots$ and see that $b(n) \to 1$. Letting $y_1 = 1$ we compute

$$c(999) = 2.000000\ldots,$$

$$c(1000) = 2.000000\ldots.$$

We see that $c(n) \to 2$. Clearly $e^{-2\pi inx}$ cannot converge to 2, thus $|z| = 1$. We easily observe that $x = 0$, thus $z = i$.

Example 6.0.10. ($\alpha = 66^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau) - 66^3} = 1 + 286752q + 82226315736q^2 + 23578503968567424q^3 + \cdots .$$

We find that $b(1) = 2.0000001\ldots$ matches the limiting value up to 6 decimal places. Letting $y_1 = 2$ we compute

$$c(1) = 1.000002\ldots,$$

$$c(2) = 1.000000001\ldots.$$

We see that $c(n) \to 1$. The size of y shows that $|z| > 1$, thus we have

$$e^{-2\pi ix} \sim c(n).$$

We easily observe that $x = 0$, thus $z = 2i$.

Example 6.0.11. ($\alpha = 20^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau) - 20^3} = 1 + 7256q + 52255768q^2 + 377674781024q^3 + \cdots .$$

We find that $b(3) = 1.414213650\ldots$ matches the limiting value up to 6 decimal places. Letting $y_1 = 1.41421365$ we compute

$$c(1) = 1.000000\ldots,$$

$$c(2) = 0.999998\ldots.$$

We see that $c(n) \to 1$. We easily observe that $x = 0$, thus $z = \sqrt{2}i$.

Example 6.0.12. ($\alpha = 2 \cdot 30^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau) - 2 \cdot 30^3} = 1 + 53256q + 2835807768q^2 + 151013228757024q^3 + \cdots .$$

We find that $b(3) = 1.73205083\ldots$ matches the limiting value up to 7 decimal places. Letting $y_1 = 1.73205083$ we compute

$$c(1) = 1.00007\ldots,$$

$$c(2) = 1\ldots.$$

We see that $c(n) \to 1$. We easily observe that $x = 0$, thus $z = \sqrt{3}i$.

Example 6.0.13. ($\alpha = -3 \cdot 160^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau) + 3 \cdot 160^3} = 1 - 12288744q + 151013228703768q^2 + \cdots .$$

We find that $b(1) = 2.59807621156\ldots$ matches the limiting value up to 9 decimal places. Letting $y_1 = 2.59807621156$ we compute

$$c(1) = -1.00002\ldots,$$
$$c(2) = 1.00005\ldots.$$

We see that $c(n) \approx (-1)^n$. The size of y shows that $|z| > 1$, thus we have

$$e^{-2\pi i x} \sim c(n).$$

We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+3\sqrt{3}i}{2}$.

Example 6.0.14. ($\alpha = -15^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+15^3} = 1 - 4119q + 16572393q^2 - 67515202851q^3 + \cdots.$$

We find that $b(3) = 1.3228756550\ldots$ matches the limiting value up to 9 decimal places. Letting $y_1 = 1.3228756550$ we compute

$$c(3) = -1.000000\ldots,$$
$$c(4) = 1.000000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{7}i}{2}$.

Example 6.0.15. ($\alpha = -32^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+32^3} = 1 - 33512q + 1122660376q^2 - 37616061025184q^3 + \cdots.$$

We find that $b(2) = 1.658312306777\ldots$ matches the limiting value up to 7 decimal places. Letting $y_1 = 1.658312306777$ we compute

$$c(1) = -1.00018\ldots,$$
$$c(2) = 1.00000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{11}i}{2}$.

Example 6.0.16. ($\alpha = -96^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+96^3} = 1 - 885480q + 784074436632q^2 - 694282057876540320q^3 + \cdots .$$

We find that $b(1) = 2.1794495\ldots$ matches the limiting value up to 6 decimal places. Letting $y_1 = 2.1794495$ we compute

$$c(1) = -1.000000\ldots,$$
$$c(2) = 1.000000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{19}i}{2}$.

Example 6.0.17. ($\alpha = -960^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+960^3} = 1 - 884736744q + 782759106183327768q^2 + \cdots .$$

We find that $b(1) = 3.27871926215104\ldots$ matches the limiting value up to 13 decimal places. Letting $y_1 = 3.27871926215104$ we compute

$$c(1) = -1.000000\ldots,$$
$$c(2) = 1.00000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{43}i}{2}$.

Example 6.0.18. ($\alpha = -5280^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+5280^3} = 1 - 147197952744q + 21667237292024856735768q^2 + \cdots .$$

We find that $b(1) = 4.09267638593622498497685\ldots$ matches the limiting value up to 13 decimal places. Letting $y_1 = 4.09267638593622498497685$ we compute

$$c(1) = -1.000000000000000009\ldots,$$
$$c(2) = 1.000000000000000000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{67}i}{2}$.

Example 6.0.19. ($\alpha = -640320^3$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)+640320^3} = 1 - 262537412640768744q + \cdots .$$

We find that $b(1) = 6.3835726674018523308554760048904\ldots$ matches the limiting value up to 30 decimal places. Letting $y_1 = 6.3835726674018523308554760048904$ we compute

$$c(1) = -1.000000000000000000000000000003\ldots,$$
$$c(2) = 1.000000000000000000000000000000\ldots.$$

We see that $c(n) \approx (-1)^n$. We easily observe that $x = -\frac{1}{2}$, thus $z = \frac{-1+\sqrt{163}i}{2}$.

Example 6.0.20. ($\alpha = 163i$) We have

$$-\frac{\Theta(j(\tau))}{j(\tau)-163i} = 1 - (744-163i)q + (133199-242544i)q^2 + \cdots .$$

We find that $b(100) = 1.00607557620624682488\ldots$. Letting

$y_1 = 1.00607557620624682489$ we compute

$$x \approx \frac{1}{2\pi}(w_{100} - w_{99}) = 0.062158154815274417\ldots,$$

thus

$$z \approx .062158154815274417 + 1.00607557620624682489i.$$

Bibliography

[1] Tom M. Apostol. *Modular functions and Dirichlet series in number theory.* Springer-Verlag, 1976.

[2] Jonathan M. Borwein and Peter B. Borwein. *Pi and the AGM: a study in analytic number theory and computational complexity.* Wiley, 1987.

[3] Jan H. Bruinier, Winfried Kohnen, and Ken Ono. The arithmetic of the values of modular functions and the divisors of modular forms. *Compositio Mathematica Compositio Math.*, 140(03):552566, 2004.

[4] Anthony W. Knapp. *Elliptic curves.* Princeton University Press, 1992.

[5] Kathrin Bringmann, Ben Kane, Steffen Löbrich, Ken Ono and Larry Rolen. On divisors of modular forms. preprint, arXiv.org:1609.08100v2, 2016.

[6] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series.* Published for the Conference Board of the Mathematical Sciences by the American Mathematical Society with support from the National Science Foundation, 2004.

[7] Joseph H. Silverman and John Torrence Tate. *Rational points on elliptic curves.* Springer-Verlag, 1992.