Hossein Movasati

A Differential Introduction to Modular Forms and Elliptic Curves

The text is under construction and it is very messy. DO NOT PRINT IT

August 8, 2019
# Contents

1 Introduction ................................................................. 3
   1.1 Fibonacci sequence ............................................. 3
   1.2 Fermat's last theorem .......................................... 4
   1.3 Arithmetic modularity theorem ............................... 5
   1.4 Beyond elliptic curves ......................................... 7
   1.5 Prerequisites .................................................... 7

2 Modular forms ............................................................. 9
   2.1 Elliptic functions ............................................... 9
   2.2 The modular group and its action ............................ 12
   2.3 Slash operator .................................................. 13
   2.4 Weierstrass $\wp$-function ................................. 14
   2.5 Differential equation of $\wp$ ............................... 16
   2.6 Eisenstein series ............................................... 17
   2.7 Fourier expansion of Eisenstein series .................... 19
   2.8 The Eisenstein series $E_2$ .................................. 22
   2.9 The algebra of modular forms ................................. 23
   2.10 Ramanujan relations between Eisenstein series .......... 24
   2.11 The product formula for discriminant .................... 25
   2.12 The $j$ function ............................................... 26
   2.13 Poincaré metric ............................................... 27
   2.14 The numbers $e_1, e_2, e_3$ ................................ 27
   2.15 Growth of coefficients ....................................... 28
   2.16 Dedekind eta function ....................................... 30
   2.17 Modular forms as k-fold differential ..................... 30
   2.18 Petersson scalar product .................................... 31
   2.19 Computing $E_2$ as a double sum ......................... 33

3 Elliptic curves and integrals ........................................ 35
   3.1 Introduction .................................................... 35
   3.2 Elliptic integrals ............................................... 35
3.3 Elliptic curves in Weierstrass format ............................................. 39
3.4 Picard-Lefschetz theory ................................................................. 39
3.5 Weierstrass uniformization theorem ............................................... 40
3.6 Sketch of the proof of Theorem (2.9.1) ........................................... 41
3.7 Some identities .............................................................................. 42
3.8 Schwarz function .......................................................................... 43
3.9 CM elliptic curves ......................................................................... 44
3.10 Fourier expansions and elliptic integrals ....................................... 44

4 Rudiments of Algebraic Geometry of curves ........................................ 47
  4.1 Curves ......................................................................................... 47
  4.2 Charts ......................................................................................... 48
  4.3 Schemes ....................................................................................... 49
  4.4 Singular and smooth curves ............................................................ 50
  4.5 Resultant and discriminant .............................................................. 50
  4.6 Discriminant ................................................................................ 51
  4.7 The main property of the discriminant ........................................... 53
  4.8 Discriminant of projective curves ................................................. 53
  4.9 Curves of genus zero ..................................................................... 54
  4.10 Curves of genus bigger than one .................................................. 54
  4.11 Elliptic curves in Weierstrass form .............................................. 55
  4.12 Elliptic curves in Weierstrass form .............................................. 55
  4.13 Real geometry of elliptic curves ................................................... 56
  4.14 Complex geometry of elliptic curves ........................................... 56
  4.15 The group law in elliptic curves ................................................... 57
  4.16 Divisors ....................................................................................... 59
  4.17 Riemann-Roch theorem ............................................................... 60
  4.18 Weierstrass form revised .............................................................. 60
  4.19 Moduli of elliptic curves .............................................................. 61
  4.20 The addition formula for \( \wp \) ..................................................... 62
  4.21 Why Schemes? ........................................................................... 64

5 Mordell-Weil Theorem ................................................................. 65
  5.1 Mordell-Weil theorem ................................................................. 65
  5.2 Weak Mordell-Weil theorem .......................................................... 71

6 Torsions and isogeny ................................................................. 73
  6.1 Torsion points .............................................................................. 73
  6.2 Isogeny ......................................................................................... 74
  6.3 Isogeny II ...................................................................................... 76

7 Hecke operators ................................................................. 77
  7.1 Hecke operators ........................................................................... 77
  7.2 Hecke and cusp forms ................................................................. 81
  7.3 Proof of Theorem 6.3.1 ................................................................. 82
# Contents

8 **Riemann zeta function** .......................... 85
  8.1 Riemann zeta function .................................. 85
  8.2 The big Oh notation .................................. 86
  8.3 Gamma function ..................................... 87
  8.4 Mellin transform .................................... 88
  8.5 Analytic extension .................................. 88
  8.6 Functional equation ................................. 89
  8.7 Second proof for functional equation ............. 90
  8.8 Zeta and primes ..................................... 91
  8.9 Other zeta functions ................................. 92
  8.10 Dedekind Zeta function ............................... 93
  8.11 L-function of cusp forms ............................. 93
  8.12 Hecke’s L-functions ................................ 94
  8.13 L-function of CY-modular forms ..................... 96

9 **Congruence groups** .................................... 99
  9.1 Congruence groups ................................. 99
  9.2 Weil pairing ....................................... 100
  9.3 Moduli spaces of elliptic curves .................. 101
  9.4 Modular forms for congruence groups ............. 101
  9.5 $q$-expansion ...................................... 102
  9.6 Transcendental degree of modular forms ......... 104

10 **Elliptic curves as Diophantine equations** ........ 107
  10.1 Finite fields ...................................... 107
  10.2 Zeta functions of elliptic curves over finite fields .......................... 107
  10.3 Nagell-Lutz Theorem ................................ 109
  10.4 Mazur theorem ..................................... 109
  10.5 One dimensional algebraic groups ................. 110
  10.6 Reduction of elliptic curves ....................... 110
  10.7 Zeta functions of curves over $\mathbb{Q}$ ............ 111
  10.8 Hasse-Weil conjecture ............................... 112
  10.9 Birch Swinnerton-Dyer conjecture .................. 113
  10.10 Congruent numbers ................................. 113
  10.11 $p$-adic numbers ................................ 117

11 **Theta series** ........................................ 119
  11.1 Two-squares theorem ................................ 122
  11.2 Poisson summation formula ......................... 123

12 **Picard curious example** ............................. 125
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Online supplemental items</td>
<td>129</td>
</tr>
<tr>
<td>13.1 Introduction</td>
<td>129</td>
</tr>
<tr>
<td>13.2 How to start?</td>
<td>129</td>
</tr>
<tr>
<td>13.3 Ramanujan differential equation</td>
<td>129</td>
</tr>
<tr>
<td>References</td>
<td>130</td>
</tr>
<tr>
<td>Index</td>
<td>133</td>
</tr>
</tbody>
</table>
Preface

There are so many books on modular forms and elliptic curves that it might seem useless to add another one. None of these books approach modular forms from the point of view of differential equations and this differentiate the present book from others. This has resulted in a tremendous generalization of modular forms whose origin partially comes from many $q$-expansion computations in theoretical physics and in particular string theory.

Hossein Movasati
January 2020
Rio de Janeiro, RJ, Brazil
Chapter 1
Introduction

Our main interest on modular forms is the fact that they are generating functions for many unexpected countings in mathematics. Why generating functions are useful might be explained with the simple example of Fibonacci numbers.

1.1 Fibonacci sequence

The Fibonacci sequence is defined in the following way

\[ F_{n+2} = F_{n+1} + F_n, \quad n \geq 0, \quad F_0 = 1, \quad F_1 = 1 \] (1.1)

Few elements of this sequence are

1, 1, 2, 3, 5, 8, 13, 21, ...

Once you have a sequence of natural numbers in mathematics, it is recommended to put it in a generating function:

\[ F(q) : = q + q^2 + 2q^3 + 3q^4 + \ldots + F_nq^n + \cdots \]

At the beginning this is just a formal power series, however, soon it will become clear that its convergence and radius of convergence carries many information of the sequence \( F_n \) itself. For now, let us do the following manipulation:

\[
F(q) = \sum_{n=0}^{\infty} F_nq^n = q + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2})q^n \\
= q + q \cdot F(q) + q^2 F(q)
\]

which implies that

\[ F(q) = \frac{q}{1-q-q^2} \] (1.2)
Therefore, $F(q)$ converges to a rational function. In order to find the radius of convergence of a rational function, we have to find the roots of its denominator:

$$F(q) = \frac{q}{1 - q - q^2} = \frac{q}{(1 - \alpha \cdot q)(1 - \beta \cdot q)} = \frac{(\alpha - \beta)^{-1}}{1 - \alpha \cdot q} - \frac{(\alpha - \beta)^{-1}}{1 - \beta \cdot q}$$

$$= \sum_{n=0}^{\infty} \left( \frac{\alpha^n - \beta^n}{\alpha - \beta} \right) q^n$$

where $\alpha = \frac{1}{2} \left( 1 + \sqrt{5} \right)$, $\beta = \frac{1}{2} \left( 1 - \sqrt{5} \right)$. We conclude that

$$F_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{\sqrt{5}}$$

Which at first glance looks strange because we have found a formula for the integer $F_n$ in terms of square root of 5. Since the radius of convergence of $F(q)$ is $\min \left\{ \frac{1}{|\alpha|}, \frac{1}{|\beta|} \right\} = \max \{|\alpha|, |\beta|\} = |\alpha|$, we conclude that

$$\lim_{n \to \infty} \frac{F_n}{F_{n-1}} = \lim_{n \to \infty} F_n^{\frac{1}{2}} = \frac{1}{2} \left( 1 + \sqrt{5} \right)$$

This number is called the golden ratio or the golden number.

**Exercise 1** Show that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

**1.2 Fermat’s last theorem**

Modular forms and elliptic curves are firmly rooted in the fertile grounds of number theory. As a proof of the mentioned fact and as an introduction to the present text we mention the followings: For $p$ prime, the Fermat last theorem ask for a non-trivial integer solution for the Diophantine equation

$$a^p + b^p + c^p = 0$$

For a hypothetical solution $(A, B, C) = (a^p, b^p, c^p)$ of the Fermat equation with $abc \neq 0$, Gerhart Frey considered the elliptic curve

$$E_{A,B,C} : y^2 = x(x-A)(x+B)$$

From this one construct a modular form $f_{A,B,C}$ and a Galois representation with certain properties and then one proves that such objects does not exist. During this passage one encounters the Modularity conjecture which claims that every elliptic
1.3 Arithmetic modularity theorem

A curve over $\mathbb{Q}$ is modular. Roughly speaking this means that every elliptic curve over $\mathbb{Q}$ appears in the Jacobian of a modular curve of level $N$. Another formulation of modularity property is by using $L$ functions which generalizes the famous Riemann zeta function

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Riemann hypothesis claims that all the non-trivial zeros of $\zeta(s)$ lies on $\Re(s) = \frac{1}{2}$ and it has strong consequences on the growth of prime number. For the $L$ functions associated to elliptic curves one has the Birch-Swinnerton Dyer conjecture which predicts the rank of an elliptic curve to be the order of vanishing of the corresponding $L$-function at $s = 1$.

1.3 Aritmetic modularity theorem

Modular forms as generating functions have many fascinating and mysterious applications. Arithmetic modularity theorem is one of these. In many books and articles we find the expression

"Let $E$ be an elliptic curve over $\mathbb{Z}$.

This has an intrinsic definition, that for now, we don’t want to get into its details.

We content ourselves with the example.

$$E: y^2 + y = x^3 - x^2$$

which the reader might consider it as a Diophantine equation, that is, we are interested to find $x$ and $y$ in the ring of integers, the field of rational numbers, finite fields, etc. Let $p$ be a prime number (don’t take the Grothendieck’s prime)\footnote{A. Grothendieck (1928-2014) is one of the founders of modern Arithmetic Algebraic Geometry. Once he was asked to give an example of a prime number and he answered: 57.} We count the number of solutions $N_p$ of $E$ modulo the prime $p$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>Solutions</th>
<th>$N_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(0,0), (0,1), (1,0), (1,1)</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>(0,0), (0,2), (1,0), (1,2)</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>(0,0), (0,4), (1,0), (1,4)</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>(0,0), (0,6), (1,0), (1,6), ( ) ,...</td>
<td>9</td>
</tr>
<tr>
<td>11</td>
<td>(0,0), (0,10), (1,0), (1,10), ( ) ,...</td>
<td>10</td>
</tr>
</tbody>
</table>

In total we have to substitute $p^2$ pairs $(x, y)$, $x, y = 0, 1, \ldots, p - 1$ inside $E$ and verify whether modulo prime $p$ it is zero or not. The first four solutions in the above table have to do with the fact that over integers $E$ has already four solutions.

$(0, 0), (0, -1), (1, 0), (1, -1)$
A priori, if we have computed $N_2, N_3, N_5, \ldots, N_{11}$, this doesn’t give any clue how to find the number $N_{13}$. We have to check $13^2$ cases again. In modern language, we say that, we are counting the number of $\mathbb{F}_p$-rational points of $E$ and we write

$$N_p : = \# E(\mathbb{F}_p)$$

Here $\mathbb{F}_p := \{0, 1, 2, \ldots, p - 1\}$ is the finite field with $p$ elements.

**Exercise 2** Find $N_p$ for all $p \leq 20$.

The theory of modular forms, and in particular arithmetic modularity theorem, says that there is a closed formula for the generating function of $N_p$’s. This is as follows. Let

$$\eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

be the Dedekind eta function. We consider it as a formal product. Let

$$F(q) = \eta(q)^2 \eta(q^{11})^2$$

$$= q^{1/2 + 2\cdot 11} \prod_{n=1}^{\infty} (1 - q^n)^2 \prod_{n=1}^{\infty} (1 - q^{11n})^2$$

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + \ldots$$

$$= \sum_{n=1}^{\infty} f_n q^n$$

The arithmetic modularity theorem tells us that

$$N_p = p - f_p$$

and $f$ is a modular form. More precisely,

“$f$ is a weight 2 new form for $\Gamma_0(11)$”

One of the aims of the present text is to understand this statement. This phenomena is a part of a general theorem:

**Theorem 1.3.1 (Arithmetic modularity theorem)** (A. Wiles, R. Taylor, C. Breuil, B. Conrad, F. Diamond) For any elliptic curve $E$ over $\mathbb{Q}$, there is a modular form $f = \sum_{n=1}^{\infty} f_n q^n$ such that (1.4) holds for all except a finite number of primes.

A precise statement, together with other equivalent versions will be presented in this text.

**Exercise 3** Show that the radius of convergence of the Dedekind $\eta$ function is 1.
1.4 Beyond elliptic curves

There is a tremendous amount of effort to generalize the arithmetic modularity theorem beyond elliptic curves. Here we give an example taken from [Schuett2013]. Let us consider the Fermat quartic surface

\[ X = X_2^4 \subseteq \mathbb{P}^3 : x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0 \]

We count the number of solutions of this Diophantine equation over the field \( \mathbb{F}_p, p \neq 2 \)

\[ \#X(\mathbb{F}_p) = \# \{(x_0 : x_1 : x_2 : x_3) \mid x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0 \} \]

Here, \([x_0 : x_1 : x_2 : x_3]\) is the equivalence class

\((x_0 : x_1 : x_2 : x_3) \sim (y_0, y_1, y_2, y_3) \iff \exists a \in \mathbb{F}_p - \{0\}\)

such that \(x_i = ay_i, \forall i = 0, 1, 2, 3\). It turns out that

\[ \#X(\mathbb{F}_p) = 1 + b_p + h \cdot p + p^2 \]

where

\[ \eta(4\tau)^6 = q \prod_{n=1}^{\infty} (1 - q^{4n})^6 = \sum_{n=1}^{\infty} b_n q^n \]

\[ h = 5 + 3\chi_{-1}(p) + 6 \cdot (\chi_2(p) + \chi_{-2}(p)) \]

and \(\chi_a(p) := (\frac{a}{p})\) is the Legendre symbol.

**Exercise 4** Verify the above affirmation for \( p = 3, 5, \ldots \) what goes wrong for \( p = 2 \)?

1.5 Prerequisites

It is assumed that the reader has a basic knowledge in algebraic geometry of curves and complex analysis in one variable.
Chapter 2
Modular forms

I have told the story before, but it is ironic that being at the same university, Artin had discovered a new type of L-series and Hecke, in trying to figure out what kind of modular forms of weight one there were, said they should correspond to some kind of L-function. The L-functions Hecke sought were among those that Artin had defined, but they never made contact—it took almost forty years until this connection was guessed and ten more before it was proved, by Langlands. Hecke was older than Artin by about ten years, but I think the main reason they did not make contact was their difference in mathematical taste. Moral: Be open to all approaches to a subject, (J. Tate in [RS11] page 446).

2.1 Elliptic functions

Definition 2.1.1 A lattice $\Lambda$ in $\mathbb{C}$ is a discrete subgroup of $(\mathbb{C}, +)$ which generate it as an $\mathbb{R}$-vector space

It follows easily that

$$\Lambda = \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2 = \{n \omega_1 + m \omega_2 | n, m \in \mathbb{Z}\}$$

where $\omega_1, \omega_2 \in \mathbb{C}$, $\omega_1, \omega_2 \neq 0$, $\text{Im}(\omega_2/\omega_1) \neq 0$. By changing the order of $\omega_1, \omega_2$, if necessary, we can assume that

$$\text{Im}(\tau) > 0, \quad \tau := \frac{\omega_1}{\omega_2}$$  \hspace{1cm} (2.1)

A lattice in general is equipped with a bilinear map $\Lambda \times \Lambda \rightarrow \mathbb{Z}$. In our case it is skew-symmetric, that is,

$$\langle a, b \rangle = -\langle b, a \rangle \quad \forall a, b \in \Lambda$$

and so $\langle \omega_1, \omega_1 \rangle = 0, \langle \omega_2, \omega_2 \rangle = 0$. Therefore,
\begin{equation}
\langle \omega_2, \omega_1 \rangle := 1 \tag{2.2}
\end{equation}
determines \langle \cdot, \cdot \rangle uniquely. The choice of \( \omega_1, \omega_2 \) with (2.1) and hence with (2.2) is also called an orientation of \( \Lambda \). If we choose another basis \( \omega_1', \omega_2' \) with (2.2) then

\[ \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, \quad A \in \text{SL}(2, \mathbb{Z}), \]

where

\[ \text{SL}(2, \mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d, \in \mathbb{Z}, \ ad - bc = 1 \right\}. \tag{2.3} \]

Let \( P \) be the space of lattice in \( \mathbb{C} \). The group

\[ \mathbb{G}_m = \mathbb{C}^* = (\mathbb{C} - \{0\}, \cdot) \tag{2.4} \]

acts on \( P \) from the right

\[ P \times \mathbb{C}^* \to P \]

\[ (A, \lambda) \mapsto A \cdot \lambda := \mathbb{Z} \omega_1 \lambda + \mathbb{Z} \omega_2 \lambda \]

For a lattice \( \Lambda \) the associate complex tori is simply

\[ E := \mathbb{C}/\Lambda \]

this means that two points \( z_1, z_2 \in \mathbb{C} \) are equivalent if \( z_1 - z_2 \in \Lambda \). The set \( \mathbb{C}/\Lambda \) is an example of a Riemann surface or complex manifold. It is called real torus of
2.1 Elliptic functions

Fig. 2.2 Torus

dimension two or complex torus of dimension one. It has the structure of an abelian group which inherits from $(\mathbb{C},+)$. Still we do not call it an elliptic curve as this name is reserved for a similar object in algebraic geometry. In mathematics when we have a space, then we start to study the set of its functions. In our case, we are interested on meromorphic functions on $\mathbb{C}/\Lambda$ as we have:

Exercise 5 There is no holomorphic function on $E$.

The pull-back of a meromorphic function by the projection map $\mathbb{C} \to E$ corresponds to a meromorphic function $f$ with

$$
\begin{align*}
  f : \mathbb{C} &\to \mathbb{C}, \\
  f(z + \omega) &= f(z) \quad \forall z \in \mathbb{C}, \ \omega \in \Lambda.
\end{align*}
$$

Since $\Lambda$ is generated by $\omega_1, \omega_2$, (2.5) is equivalent to

$$
\begin{align*}
  f(z + \omega_1) &= f(z) \\
  f(z + \omega_2) &= f(z) \quad \forall z \in \mathbb{C},
\end{align*}
$$

that is $f$ is double periodic. We may also view $f$ as a function in both $z \in \mathbb{C}$ and $\Lambda \in P$. In this case we write $f(z) = f(z, \Lambda)$. Since $P$ is equipped with a $\mathbb{C}^*$-action, it is natural to characterize functions $f$ with

$$
\begin{align*}
  f(\lambda z, \lambda \Lambda) = \lambda^{-a} f(z, \Lambda), \forall \lambda \in \mathbb{C}^* \quad (2.5)
\end{align*}
$$

for some fixed $a \in \mathbb{Z}$. 
Definition 2.1.2 A meromorphic function $f$ with the property \( (2.5) \) is called an elliptic function (of weight $a$).

Let us consider an elliptic function $f$ and write its Laurent series at $z = 0$,

$$f(z, \Lambda) = \sum_{n=-\infty}^{+\infty} f_n(\Lambda) z^n$$

The coefficients $f_n(\Lambda)$ are functions of the lattice $\Lambda$ and it is easy to see that \( (2.5) \) is equivalent to the following functional equations for $f_n(\Lambda)$’s

$$f_n(\lambda \Lambda) = \lambda^{-a-n} f_n(\Lambda) \quad \forall \lambda \in \mathbb{C}^*.$$

This is as follows

$$f(\lambda z, \lambda \Lambda) = \sum_{n=-\infty}^{+\infty} f_n(\lambda \Lambda)(\lambda z)^n$$

$$= \lambda^{-a} \left( \sum_{n=-\infty}^{+\infty} f_n(\Lambda) z^n \right)$$

Definition 2.1.3 A meromorphic function $f$ on the space $P$ of lattices is called a meromorphic modular form of weight $n \in \mathbb{Z}$ if

$$f(\lambda \Lambda) = \lambda^{-n} f(\Lambda) \quad \forall \lambda \in \mathbb{C}^*, \Lambda \in P.$$

Therefore, from a meromorphic elliptic function of weight $a$ we get meromorphic modular form $f_n$ of weight $n+a$. If we evaluate a meromorphic modular form $f$ of weight $n$ on lattices $\Lambda = \mathbb{Z} \tau + \mathbb{Z}$ with $\tau$ in the upper half plane $\mathbb{H}$ and regard them as a function in $\tau$, we get a meromorphic function $f$ in $\mathbb{H}$ with the following functional equation.

$$(c \tau + d)^{-n} f\left(\frac{a \tau + b}{c \tau + d}\right) = f(\tau), \quad \forall \tau \in \mathbb{H}. \quad (2.6)$$

2.2 The modular group and its action

The upper half plane is defined as

$$\mathbb{H} := \{ \tau \in \mathbb{C} | \text{Im}(\tau) > 0 \}.$$

The following group acts on $\mathbb{H}$ by Möbius transformation
2.3 Slash operator

$$\text{SL}(2, \mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1, a, b, c, d, \in \mathbb{R} \right\}$$

$$\text{SL}(2, \mathbb{R}) \times \mathbb{H} \longrightarrow \mathbb{H}$$

$$(A, \tau) \longrightarrow A\tau := \frac{a\tau + b}{c\tau + d}$$

where $$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{R})$$. This follows from

$$\text{Im}(A\tau) = \frac{\text{Im}(\tau) \det(A)}{|c\tau + d|^2} \quad (2.7)$$

An element $$A \in \text{SL}(2, \mathbb{R})$$ acts as identity on $$\mathbb{H}$$ if it is $$\pm I$$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is the identity matrix. Therefore, it is useful to define

$$\text{PSL}(2, \mathbb{R}) = \text{SL}(2, \mathbb{R}) / \pm I$$

The protagonist of the present text is the group $$\text{SL}(2, \mathbb{Z})$$ defined in (2.3). Let $$\tau \in \mathbb{H}$$ and assume that it has non-trivial stabilizer under the action of $$\text{SL}(2, \mathbb{Z})$$, that is, there is $$A \in \text{SL}(2, \mathbb{Z})$$, $$A \neq \pm I$$ such that $$A\tau = \tau$$. Since $$\det A = +1$$ and $$\text{Im}(\tau) > 0$$ we get $$|a + d| < 2$$ and $$\tau = \frac{a - d + \sqrt{(a + d)^2 - 4}}{c}$$.

**Exercise 6** Show that the group $$\text{SL}(2, \mathbb{Z})$$ is generated by

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (2.8)$$

**2.3 Slash operator**

For $$A \in \text{GL}(2, \mathbb{R})$$ and a modular form $$f$$ of weight $$k$$ we define the slash operator

$$f|_k A := (\det A)^{k-1}(c\tau + d)^{-k}f(A\tau), \quad A = \begin{pmatrix} * & * \\ c & d \end{pmatrix}.$$ 

In some books, the power $$k - 1$$ of $$\det A$$ is different. For instance, in Chapter [7] the slash operator is different. For $$A \in \text{SL}(2, \mathbb{R})$$ this will not make any difference.

**Proposition 2.3.1** If $$B \in \text{GL}(2, \mathbb{R})$$ and $$f$$ is a meromorphic modular form of weight $$k$$ for some group $$\Gamma \in \text{GL}(2, \mathbb{R})$$ then $$f|_k B$$ is a modular form of the same weight for $$B^{-1}\Gamma B$$.

**Proof.** This follows from
(f|_kB)|_kB^{-1}AB = (f|_kA)|_kB = f|_kB

\[\square\]

2.4 Weierstrass \(\wp\)-function

When a discrete group \(\Gamma\) acts on a space \(M\) and we want to construct functions on the quotient space

\[\Gamma \setminus M := M/\sim \quad x \sim y \iff x = Ay \quad \text{for some } A \in \Gamma\]

the first receipe is to start with a function \(\tilde{f}\) on \(M\) and define the formal sum

\[f(\tau) = \sum_{A \in \Gamma} \tilde{f}(A\tau)\quad (2.9)\]

If we don’t care about the convergence of \(f\), the we can check that it is invariant under the action of \(\Gamma\). For any \(B \in \Gamma\) we have

\[f(B\tau) = \sum_{A \in \Gamma} \tilde{f}(AB\tau) = \sum_{A \in \Gamma} \tilde{f}(A\tau) = f(\tau)\]

Note that we have used the fact that the multiplication by \(B\) from the right induces a bijection \(\Gamma \rightarrow \Gamma\). We get the function

\[\tilde{f} : \Gamma \setminus M \rightarrow \mathbb{C}, \quad \tilde{f}([\tau]) = f(\tau)\]

which we denot it again by \(f = \tilde{f}\) If \(\Gamma\) is finite then (2.9) is a finite sum an so \(f\) is well-defined, however, in general such a sum might not be convergent. In Our case, the lattice \(\Lambda\) as an additive group acts on \(\mathbb{C}\)

\[\Lambda \times \mathbb{C} \rightarrow \mathbb{C}, (\lambda, z) \mapsto z + \lambda\].

**Theorem 2.4.1** Show that the number of zeros of a non-constant elliptic function counted in \(\mathbb{C}/\Lambda\) is equal to the number of poles, counted with multiplicity, and it is bigger than or equal to 2.

**Proof.** See [Apostol 1989], page 5-6.

For our purpose we start with \(\tilde{f}(z) = z^{-a}, a \in \mathbb{Z}\) and define
2.4 Weierstrass $\wp$-function

\[ f_a(z) = f_a(z, \omega) = \sum_{\omega \in \Lambda} (z + \omega)^{-a} \]
\[ = \sum_{(n,m) \in \mathbb{Z}^2} (z + n\omega_1 + m\omega_2)^{-a} \]

**Proposition 2.4.1** The infinite series $f_a(z)$ converges absolutely for $a \in \mathbb{N}$ with $a \geq 3$

**Proof.** (See lemma 2 page 8 of [Apostol]). We can assume that the sum is taken for all $\omega \in \Lambda, |\omega| > R$ and $|z| < R$. There is a constant $M$ depending on $R$ and $a$ such that

\[ \frac{1}{|z - \omega|^a} \leq \frac{M}{|\omega|^a} \quad \forall \omega \in \Lambda, |\omega| > R \]
\[ \forall z \in \mathbb{C}, |z| < R \]

Therefore, it is enough to prove that the sum $\sum_{\omega \in \Lambda} \frac{1}{|\omega|^a}$ is convergent. Let $r$ and $R$ be the minimum and maximum distance of 0 from the parallelogram formed by $\pm \omega_1 \pm \omega_2$. Then the parallelogram $P_n$ formed by four vertices $n(\pm \omega_1 \pm \omega_2)$ has the minimum and maximum distances $nr$ and $nR$, respectively, from 0. Moreover, it has $8n$ points of the lattice. Therefore, the sum $S_n$ corresponding to all parallelograms $P_1, P_2, \ldots, P_n$ satisfies

\[ \frac{8}{R^a}(1 + 2^{a-1} + \cdots + n^{a-1}) \leq S_n \leq \frac{8}{r^a}(1 + 2^{a-1} + \cdots + n^{a-1}) \]

\[ \square \]

**Exercise 7** Show that $f_2$ does not converge in any $z \in \mathbb{C}, z \notin \Lambda$

Note that

\[ \frac{\partial f_a}{\partial z} = -a \cdot f_{a+1} \]

**Definition 2.4.1** The Weierstrass $\wp$ function (read P) is

\[ \wp(z, \Lambda) = \wp(z) := \frac{1}{z^2} + \sum_{\omega \neq 0} \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \]

**Proposition 2.4.2** $\wp$ is convergent

**Proof.** (See [Apostol] Theorem 1.10). We have

\[ \left| \frac{1}{(z - \omega)^a} - \frac{1}{\omega^a} \right| = \left| \frac{z(2\omega - z)}{(z - \omega)^a \omega^a} \right| \leq \frac{M R (2|\omega| + R)}{|\omega|^a |(\omega)^a|} \]
\[ \leq \frac{M R (2 + R/|\omega|)}{|\omega|^a} \leq \frac{3MR}{|\omega|^a} \]

where we used the notation in the proof Proposition (2.4.2) \[ \square \]
It is easy to see that

\[ \wp(-z) = \wp(z) \]

that is \( \wp \) is an even function.

**Exercise 8** Show that there is no function \( f(\omega), \omega \in \Lambda \) such that

\[ \sum_{\omega \in \Lambda} \frac{1}{z - \omega} + f(\omega) \]

is convergent.

The function \( \wp \) has poles at the points of \( \Lambda \). We write the Laurent expansion of \( \wp \) at \( z = 0 \).

**Theorem 2.4.2** We have

\[ \wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1)G_{2n+2} \cdot z^n \]

where

\[ G_{2n+2} = \sum_{\omega \neq 0} \frac{1}{\omega^{2n+2}}. \] (2.10)

and

\[ 0 < |z| < r := \min\{|\omega| \mid \omega \neq 0\}. \] (2.11)

**Proof.** For \( z \) in (2.11) we have \( \left| \frac{z}{\omega} \right| < 1 \) and

\[ \frac{1}{(z - \omega)^2} = \frac{1}{\omega^2(1 - z/\omega)^2} = \frac{1}{\omega^2} \left( 1 + \sum_{n=1}^{\infty} (n+1) \left( \frac{z}{\omega} \right)^n \right) \]

and so

\[ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty} \frac{n+1}{\omega^{n+2}} \cdot z^n \]

Summing over \( \omega \in \Lambda, \omega \neq 0 \), we get the result. \( \square \)

The notation

\[ g_2 = 60G_4, \quad g_3 = 140G_6 \] (2.12)

is frequently used.

### 2.5 Differential equation of \( \wp \)

**Theorem 2.5.1** The function \( \wp \) satisfies the differential equation

\[ \wp'(z)^2 = 4\wp(z)^3 - 60G_4z - 140G_6 \] (2.13)
Proof. Let \( f(z) \) be the difference of both sides of (2.13). This is clearly an elliptic function with possible poles at \( z \in \Lambda \). We show that \( f \) is holomorphic at \( z = 0 \) and so \( f = 0 \). We have

\[
\wp'(z) = \frac{-z^2}{4} + 6G_3 \cdot z + 20G_6 \cdot z^3 + \ldots
\]
\[
\wp'(z)^2 = \frac{z^4}{4} - 24G_4 \cdot z - 80G_6 + \ldots
\]
\[
4\wp(z)^3 = \frac{z^4}{4} + 36G_4 \cdot z + 20G_6 + \ldots
\]
hence

\[
\wp'(z)^2 = 4\wp(z)^3 = -\frac{60G_4}{z^2} - 140G_6 + \ldots
\]
\[
\wp'(z)^2 = 4\wp(z)^3 = +60G_4 \wp(z) = -140G_6 + \ldots \quad \Box
\]

**Definition 2.5.1** An elliptic function \( f \) is a meromorphic function in \( \mathbb{C} \) such that it is double periodic, that is, there are two \( \mathbb{Z} \) linearly independent complex numbers \( \omega_1, \omega_2 \in \mathbb{Z} \) such that

\[
f(z + \omega_1) = f(z), \quad f(z + \omega_2) = f(z)
\]

If \( f \) is a non-constant elliptic function, we can easily see that \( \text{Im}(\omega_1 / \omega_2) \neq 0 \).

**Exercise 9** ([Apostol] page 23, Exercise 5) Prove that every elliptic function \( f \) can be written as

\[
R_1[\wp(z)] + \wp'(z)R_2[\wp(z)]
\]

where \( R_1, R_2 \) are rational functions and \( \wp \) has the same set of periods as \( f \).

**Exercise 10** ([Apostol] page 24, Exercise 9)

\[
\wp(2z) = \frac{(\wp(z)^2 + \frac{1}{4}g_2)^2 + 2g_3 \cdot \wp(z)}{4\wp'(2z) - g_2 \wp'(z) - g_3}
\]
\[
= -2\wp(z) + \frac{1}{4} \left( \frac{\wp''(z)}{\wp'(z)} \right)^2
\]

**Exercise 11** Show that

\[
\wp''(z) = 6\wp(z) - \frac{1}{2}g_2
\]

Can you compute \( \wp''(z) \) in terms of \( \wp(z), \wp'(z) \)

### 2.6 Eisenstein series

The series

\[
G_n := \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^n}, \quad n \text{ even, } n \geq 4
\]

are called Eisenstein series. From the convergence of \( \wp \) we can derive the convergence of \( G_n \)'s. They satisfy
we usually define

\[ G_n(\tau) = G_n(\mathbb{Z}\tau + \mathbb{Z}) = \sum_{(a,b) \in \mathbb{Z}^2, (a,b) \neq (0,0)} \frac{1}{(a+b\tau)^n}, \quad \tau \in \mathbb{H} \]  

**Exercise 12** Show that \( G_2 \) doesn’t converge at any point \( \tau \in \mathbb{H} \). Show also that \( G_n \equiv 0 \), for \( n \) an odd number.

From the functional equation (2.14) we deduce the following: For all \( A \in \text{SL}(2,\mathbb{Z}) \)

\[ G_n(A\tau) = G \left( \frac{a\tau + b}{c\tau + d} \right) = G \left( \frac{a\tau + b}{c\tau + d} \right) + \mathbb{Z} + \mathbb{Z} \]  

Later we will see that

\[ \lim_{\text{Im}(\tau) \to \infty} G_n(\tau) \text{ exist} \]  

This motivate us to define (holomorphic) modular forms.

**Definition 2.6.1** Let \( k \in \mathbb{Z} \) be an integer and \( f \) be a meromorphic function on the upper half plane. Then \( f \) is called a meromorphic modular form for the subgroup \( \Gamma \subseteq \text{SL}(2,\mathbb{R}) \) if

\[ (c\tau + d)^{-k}f \left( \frac{a\tau + b}{c\tau + d} \right) = f(\tau) \quad \forall \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma \]  

Let us assume that \( \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \in \Gamma \). Then

\[ f(\tau + 1) = f(\tau) \]  

Therefore, \( f \) defines a meromorphic function \( g \) in the punctured disc:

\[ D^* = z \in \mathbb{C} \mid |z| < 1 \setminus \{ 0 \} \]  

which is defined by

\[ f(\tau) = \tilde{f}(q), \text{ where } q := e^{2\pi i \tau} \]  

The map \( \mathbb{H} \to D^* \) is depicted in Figure *( )

We write the laurent expansion of \( \tilde{f} \) at \( q = 0 \).
2.7 Fourier expansion of Eisenstein series

We know that the Eisenstein series are weakly holomorphic modular forms. In this section we show that they are holomorphic at $i\infty$ and so they are modular forms. The computation in this section can be found in [koblitz] page 110, [Apostol] page 18, Serre page 91.

Recall the Bernoulli numbers

\[ \frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \cdot \frac{x^k}{k!} \]
For instance, \( B_0 = 1, B_1 = \frac{-1}{2}, B_2 = \frac{1}{12}, B_4 = \frac{-1}{30}, B_6 = \frac{1}{42} \)

It is easy to see that for any odd \( k \geq 3 \) we have \( B_k = 0 \)

**Theorem 2.7.1** The Eisenstein series \( G_k \) has the following \( q \)-expansion

\[
G_k = 2\zeta(k) \left( 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n \right)
\]

where \( \zeta(k) := \sum_{n=1}^{\infty} \frac{1}{n^k} \) is the Riemann's zeta function and

\[
\sigma_a(n) := \sum_{d|n} d^a.
\]

We follow [Koblitz] page 110. Let us first state the main ingredient of the proof of Theorem 2.7.1

**Proposition 2.7.1** We have

\[
zeta(k) = -\left(\frac{2\pi i}{k}\right)^k B_k \frac{1}{k!} \quad k \text{ even } \geq 2 \quad (2.17)
\]

\[
\sum_{n \in \mathbb{Z}} \frac{1}{(a+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=0}^{\infty} n^{k-1} e^{2\pi i a}, \quad k \in \mathbb{N}, \quad k \geq 2, \quad a \in \mathbb{C} - \mathbb{Z} \quad (2.18)
\]

**Proof.** We have the following product formula for sine function

\[
\sin(\pi a) = \pi a \prod_{n=1}^{\infty} \left( 1 - \frac{a^2}{n^2} \right), \quad a \in \mathbb{C} \quad (2.19)
\]

Take the logarithmic derivative if (2.19) and we have

\[
\pi \cdot \cot(\pi a) = \frac{1}{a} + \sum_{n=1}^{\infty} \left( \frac{1}{a+n} + \frac{1}{a-n} \right), \quad (2.20)
\]

The left hand side of this is

\[
\pi \cdot \cot(\pi a) = \pi \frac{e^{\pi ia} + e^{-\pi ia}}{e^{\pi ia} - e^{-\pi ia}} = \pi i + \frac{2\pi i}{e^{2\pi ia} - 1}
\]

\[
= \pi i - 2\pi i \left( \sum_{n=0}^{\infty} e^{2\pi i a} \right) \quad (2.21)
\]

In (2.20) multiply both side with \( a \) and set \( x := 2\pi ia \).
2.7 Fourier expansion of Eisenstein series

\[
\frac{x}{2} + \frac{x}{e^x - 1} = 1 + \sum_{n=1}^{\infty} \frac{x}{(x+2\pi in)} + \frac{x}{(x-2\pi in)}
\]

\[
= 1 + \sum_{n=1}^{\infty} \frac{x}{2\pi in} \left( \sum_{k=0}^{\infty} \left( \frac{-x}{2\pi in} \right)^k - \left( \frac{x}{2\pi in} \right)^k \right)
\]

\[
= 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1, k \text{ odd}}^{\infty} \frac{x^{k+1}}{(2\pi in)^{k+1}}
\]

\[
= 1 - 2 \sum_{k=1, k \text{ odd}}^{\infty} \frac{x^{k+1}}{(2\pi i)^{k+1} \zeta(k+1)}
\]

We get the well-known formula (2.17). We differentiate (2.20) and (2.21) with respect to \( a \), \( k - 1 \) times, and we get

\[
(-1)(-2)\ldots(-k+1) \sum_{n \in \mathbb{Z}} \frac{1}{(a+n)^k} = -(2\pi i)^k \sum_{n=0}^{\infty} n^{k-1} e^{2\pi in a}
\]

which is (2.18).

**Proof (of Theorem 2.7.1).** Take \( a = m \tau, m \in \mathbb{Z}, m \neq 0 \), and we have

\[
\sum_{n \in \mathbb{Z}} \frac{1}{(m \tau + n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^m
\]

The result follows immediately:

\[
G_k = 2 \zeta(k) + 2 \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m \tau + n)^k}
\]

\[
= 2 \zeta(k) \left( 1 + \frac{(-2\pi i)^k}{\zeta(k)(k-1)!} \sum_{m,n=1}^{\infty} n^{k-1} q^m \right) \quad \square (2.23)
\]

We know that the Eisenstein series \( G_k \) for \( k \geq 3 \) and odd number is identically zero and hence the equality (2.22) is valid for \( k \geq 3 \) an even number. However, note that the equality (2.23) is valid also for \( k \geq 3 \) an odd number. In this case the number \( \frac{\pi^k}{\zeta(k)} \) is conjecturally a transcendental number. For this reason we may take (2.22) as the definition of \( G_k \) which works also for odd \( k \geq 3 \).

**Exercise 13.** Describe the functional equation of \( G_k(\tau), k \geq 3 \) under the action of \( SL(2, \mathbb{Z}) \). See the Master thesis of H. Bachmann.

**Exercise 14** Prove the product formula for sine in (2.19). Hint: both side have the same zero set.

We will use the following new notation
\[ E_k = G_k / 2 \zeta(k) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \] (2.24)

\[ E_4 = 1 + 240 \left( \sum_{n=1}^{\infty} \sigma_3(n) q^n \right) \] (2.25)

\[ E_6 = 1 - 504 \left( \sum_{n=1}^{\infty} \sigma_5(n) q^n \right) \] (2.26)

\[ E_8 = 1 + 480 \left( \sum_{n=1}^{\infty} \sigma_7(n) q^n \right) \] (2.27)

2.8 The Eisenstein series \( E_2 \)

We follow Koblitz p. 112. We define

\[ G_2(\tau) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m \tau + n)^2} \]

Where \( ' \) means that if \( m = 0 \) then \( n \neq 0 \). The arguments in \( \S 2.7 \) shows that the inner sums converge for any \( m \) and \( \tau \in \mathbb{H} \) and then the other sum converges. Here, the order of summation is important.

**Exercise 15** Show that the double sum

\[ \sum_{(n,m) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(m \tau + n)^2} \]

doesn’t converge.

In a similar way as in \( \S 2.7 \) we get

\[ G_2(\tau) = 2 \zeta(2) E_2(\tau), \ E_2(\tau) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n \]

**Proposition 2.8.1** We have

\[ (c \tau + d)^{-2} E_2 \left( \frac{a \tau + b}{c \tau + d} \right) - E_2(\tau) = \frac{12}{2 \pi i} \frac{c}{c \tau + d} \] (2.28)

for all \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \)

**Proof.** First we note that if we define

\[ f \|_2 A := (c \tau + d)^{-2} f(\tau) - c (c \tau + d)^{-1} \]
for a holomorphic function $f$ on $\mathbb{H}$ then
\[(f \parallel_2 A) \parallel_2 B = f \parallel_2 AB\]

Since $\text{PSL}(2, \mathbb{Z})$ is generated by $T$ and $S$ and the \((2.28)\) is trivial for $T$, it is enough to verify \((2.28)\) for $S$, that is
\[\tau^{-2}E_2 \left( \frac{-1}{\tau} \right) = E_2(\tau) + \frac{12}{2\pi i} \frac{1}{\tau}\]

$\square$

### 2.9 The algebra of modular forms

**Theorem 2.9.1** The Eisenstein series $E_4$ and $E_6$ are algebraically independent over $\mathbb{C}$, that is, there is no polynomial $P(X, Y)$ with coefficients in $\mathbb{C}$ such that $P(E_4, E_6) = 0$. Moreover any holomorphic modular form $f$ of weight $k$ can be written uniquely as
\[f = P(E_4, E_6)\]
where $P$ is a homogeneous polynomial of degree $k$ in the ring
\[\mathbb{C}[X, Y], \text{ weight } (X) = 4, \text{ weight } (Y) = 6\]  
\[(2.29)\]

There is a classical proof of Theorem (2.9.1) which can be found in almost all books on modular forms. In §3.6 we will give a new proof which is inspired by the author’s study of the generalized period domain in [Movasati2008]. The proof is based on the study of elliptic integrals and Gauss-Manin connection.

Note that a homogeneous polynomial $P$ of degree $k$ in the ring \((2.29)\) is of the form
\[P(X, Y) = \sum_{4i+6j=k} a_{i,j}X^iY^j \quad a_{i,j} \in \mathbb{C}, \quad i, j \in \mathbb{N}_0\]
and so $P(X, Y)$ is clearly a modular form of weight $k$ for $\text{SL}(2, \mathbb{Z})$. Let
\[M = M(\text{SL}(2, \mathbb{Z})) := \oplus_{k \in \mathbb{Z}} M_k\]
be the algebra of modular forms. By Theorem (2.9.1), for $k \in \mathbb{Z}$, $k \leq 2$ or $k$ odd we have $M_k = 0$ and
\[M = \mathbb{C}[E_4, E_6], \quad M_k = \mathbb{C}[E_4, E_6]_k\]
weight $(E_4) = 4$, weight$(E_6) = 6$

**Exercise 16** Show that
\[E_4^2 = E_8, \quad E_4E_6 = E_{10}, \quad E_6E_8 = E_{14}\]
and derive the corresponding equalities for $6_k(n)$. For instance

$$6_7(n) = 6_3(n) + 120 \sum_{m=1}^{n-1} 6_3(n-m)$$

The dimension of the space of modular forms $M_k$ is listed below:

<table>
<thead>
<tr>
<th>$k$</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
<th>16</th>
<th>18</th>
<th>$k$</th>
<th>$k+12$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\dim M_k$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>d</td>
<td>d+1</td>
</tr>
</tbody>
</table>

Note that

$$\dim M_k = \# \{(x, y) \in \mathbb{N}^2 / 4x + 6y = k\}$$

It is easy to see that

$$\sum_{k=0}^{m} \dim M_k q^k = \frac{1}{(1-q^4)(1-q^6)}.$$  \hspace{1cm} (2.30)

### 2.10 Ramanujan relations between Eisenstein series

The derivation of a modular form with respect to $\tau$ is no more a modular form. Instead, we have

**Proposition 2.10.1** We have the following map

$$M_k \to M_{k+2}, \ f \mapsto \frac{\partial f}{\partial \tau} - \frac{k}{12} E_2 \cdot f.$$  \hspace{1cm} (2.31)

which is called the Serre derivative of $f$

**Proof.** Let $g$ be the Serre derivative of $f$. We have to show that $g \in M_{k+2}$. Only the functional equation of $g$ is non-trivial:

$$g(A\tau) = f'(A\tau) - (2\pi i)^k \frac{k}{12} f(A\tau) E_2(A\tau)$$

$$= \cdots$$

$$= (c\tau + d)^{k+2} \cdot f(\tau)$$

for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$.

We have

$$\frac{\partial}{\partial \tau} := 2\pi i q \frac{\partial}{\partial q}.$$  

and sometime it is useful to divide the Serre derivative over $2\pi i$ and redefine it

$f \mapsto q \frac{f}{\partial q} - \frac{k}{12} E_2 f$.

**Proposition 2.10.2** we have the following equalities between Eisenstein series and their derivatives
2.11 The product formula for discriminant

\[
\begin{cases}
q \frac{\partial E_2}{\partial q} = \frac{1}{12}(E_2^3 - E_4) \\
q \frac{\partial E_4}{\partial q} = \frac{1}{4}(E_2 E_4 - E_6) \\
q \frac{\partial E_6}{\partial q} = \frac{1}{2}(E_2 E_6 - E_4^2)
\end{cases}
\]

(2.32)

Proof. The proof of the second and third equality follows from the Serre derivative. The proof of the first equality follows in a similar way. We need to prove that \( f(\tau) := -\frac{12}{2\pi i} \frac{\partial E_2}{\partial \tau} + E_2^2 \) is a modular form of weight 4 and its constant term is 1. Therefore, by Theorem 2.9.1 it must be \( E_4 \). \( \square \)

2.11 The product formula for discriminant

Recall that

\[
\zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945},
\]

We define

\[
\Delta := t_2^3 - 27t_3^2 = (2\zeta(4)60E_4)^3 - 27(2\zeta(6)140)^2E_6^2 = \frac{(2\pi)^{12}}{1728}(E_4^3 - E_6^2)
\]

and we have

\[
(2\pi)^{-12}\Delta = \frac{1}{1728}(E_4^3 - E_6^2) = \sum_{n=1}^{\infty} \tau(n)q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots =
\]

\( \tau(n) \) is called the Ramanujan function of \( n \).

Proposition 2.11.1 We have

\[
\frac{1}{1728}(E_4^3 - E_6^2) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}
\]

(2.33)

Proof. This follows from Ramanujan relations between Eisenstein series. The logarithmic derivative of both sides in (2.33) is \( E_2 \). \( \square \)

Exercise 17 ([Koblitz] III, §2.4)

1. Show that

\[
E_{12} - E_6^2 = \frac{(2\pi)^{-12} \cdot 2^6 \cdot 3^5 \cdot 7^2}{691} \cdot \Delta
\]

2. From this derive an expression for \( \tau(n) \) in terms of \( \sigma_{11} \) and \( \sigma_5 \)

3. Show that

\[
\tau(n) \equiv \sigma_{11}(n) \pmod{691}
\]
The following was conjectured by Ramanujan and proved by Deligne in [Deligne] as a by-product of his proof of the Weil conjectures.

**Theorem 2.11.1** We have
\[ |\tau(n)| < n^{11/12} \sigma(n), \]
where \( \sigma_0(n) \) is the number of divisors of \( n \).

Another interesting function is
\[ F(q) := \frac{1728 \cdot q}{E_4^3 - E_6^2} = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)} = \sum_{n=0}^{\infty} P_n q^n \]
It can be easily checked that \( P_n \) is the unrestricted partition function, that is, \( P_n \) is the number of ways a positive integer \( n \) can be expressed as a sum of positive integers:
\[ n = a_1 + a_2 + \cdots + a_k, \quad a_k \in \mathbb{N}. \]
There is no restriction on \( k \), order of \( a_i \)'s, and repetition of \( a_i \)'s is allowed. For more information see Apostol’s book [Apostol] Chapter 5.

### 2.12 The \( j \)-function

The following
\[ j(\tau) = 1728 - \frac{3}{t_2^2 - 27t_3^2} = \sum_{n=1}^{\infty} c_n q^n \]
\[ = 1728 \frac{E_4^3}{E_4^3 - E_6^2} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots \]
is called the \( j \)-function, or Klein’s modular function. It is holomorphic in \( \mathbb{H} \) and has a pole of order one at \( i\infty \). From the functional equation of Eisenstein series it follows that \( j \) is invariant under the action of \( \text{SL}(2,\mathbb{Z}) \):
\[ j \left( \frac{a \tau + b}{c \tau + d} \right) = j(\tau), \quad \forall \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{SL}(2,\mathbb{Z}). \quad (2.34) \]

**Theorem 2.12.1** The map \( j : \text{SL}(2,\mathbb{Z}) \backslash \mathbb{H} \rightarrow \mathbb{C} \) is one to one and surjective.

There is a beautiful history behind the \( j \)-function. According to [Apostol], Berwick in 1916 calculated the first seven coefficients of \( j \), Zuckerman the first 24 in 1939, and Van Wijngaarden the first 100 in 1953. The only reason for computing such numbers, seems to be only the joy of playing with them and their mysteriousness. In [Apostol] we find also some divisibility properties of \( c_n \)'s due to D.H. Lehmer in 1942 and J. Lehner in 1949. An asymptotic formula due to Petersson in 1932 and Rademacher in 1932 is also reported in [Apostol].
In 1978 MacKay noticed that $196884 = 196883 + 1$ and 196883 is the number of dimensions in which the Monster group can be most simply represented. Based on this observation J.H. Conway and S.P. Norton in 1979 formulated the Monstrous moonshine conjecture which relates all the coefficients in the $j$-function to the representation dimensions of the Monster group. In 1992 R. Borcherds solved this conjecture and got fields medal, see [Gan06] for more information on this conjecture. There proof does not give any clue why elliptic curves must have something to do with the Monster group, and so the mystery involved around it still exists. For instance, in a private conversation J.H. Conway expressed the fact that the proof for him is not satisfactory.

2.13 Poincaré metric

In the upper half plane $\mathbb{H}$ one usually use the Poincaré metric:

$$ds = \frac{dx \otimes dx + dy \otimes dy}{y} = \text{Im}(\omega), \quad \omega := \frac{dz \otimes d\bar{z}}{\text{Im}(z)}$$

$\omega$ is called the Hermitian form.

**Exercise 18** The Poincaré metric is invariant under the action of SL$(2, \mathbb{R})$. Hint: Show that

$$d(Az) \otimes d(\overline{Az}) = \frac{dz \otimes d\bar{z}}{\text{Im}(z)}$$

The volume form of the Poincaré metric is given by the imaginary part of $\omega$:

$$dV = \text{Im}(\omega) = \frac{-dx \otimes dy + dy \otimes dx}{y} = \frac{dz \wedge d\bar{z}}{-2i \text{Im}(z)}$$

We use the Poincaré metric to prove the convergency of Eisenstein series.

2.14 The numbers $e_1, e_2, e_3$

The following functions are defined in [Apostol]

$$e_1 := \wp \left( \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2, \frac{\omega_1}{2} \right)$$

$$e_2 := \wp \left( \mathbb{Z} \omega_1 + \mathbb{Z} \omega_3, \frac{\omega_1}{2} \right)$$

$$e_3 := \wp \left( \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2, \frac{\omega_1 + \omega_2}{2} \right)$$

**Proposition 2.14.1** The numbers $e_1, e_2, e_3$ are distinct and we have
4\wp(z) - g_2 \cdot \wp(z) - g_3 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) \quad (2.35)

**Proof.** Since \(\wp(z)\) is even, \(\wp'(z)\) is odd. Therefore,

\[-\wp'(1/2) = \wp'\left(-\frac{1}{2}\omega\right) = \wp'\left(\omega - \frac{1}{2}\omega\right) = \wp'\left(\frac{1}{2}\omega\right) \quad \forall \omega \in \Lambda\]

This implies that \(\omega_1, \omega_2, \omega_1 + \omega_2\) are roots of \(\wp'(z)\). The function \(\wp'(z)\) has a pole of order 3 at \(z = 0 \in \bar{E}\) and so the mentioned three points are simple roots of \(\wp'(z)\). The differential equation of \(\wp(z)\), implies that \(e_1, e_2, e_3\) are roots of the left hand side of 2.35. Now \(e_1, e_2, e_3\) are distinct. We show that \(e_1 \neq e_2\). The elliptic function \(\wp(z) - e_i\) has a double root at \(\frac{\omega_i}{2}\), because \(\wp'(\frac{1}{2}\omega_i) = 0\), all these for \(i = 1, 2, 3\) if \(e_1 = e_2\) then this function must have pole order \(\geq 4\) at \(z = 0\), which is a contradiction. \(\square\)

Now let us regard \(e_i\)'s as functions in \(\tau \in \mathbb{H}\) and redefine

\[e_1 = e_1\left(Z\tau + Z, \frac{\tau}{2}\right), \quad e_2 = e_2\left(Z\tau + Z, \frac{1}{2}\right), \quad e_3 = e_3\left(Z\tau + Z, \frac{\tau + 1}{2}\right)\]

and consider them as holomorphic functions in \(\tau\). [PUT HERE \(t_1, t_2, t_3\) of Darboux-Halphen, We have \(t_i = e_i + g_1\) \(i = 1, 2, 3\), See [Quasi-Moduler forms, I]].

### 2.15 Growth of coefficients

We follow [Serre].

**Theorem 2.15.1 (Hecke)** If \(f\) is a holomorphic cusp form for a group \(SL(2, \mathbb{Z})\) of weight \(k\) then

\[f_n = O(n^k)\]

where \(f = \sum_{n=1}^{\infty} f_n q^n\) is the \(q\)-expansion of \(f\).

**Proof.** Cauchy residue formula implies that

\[f_n = \frac{1}{2\pi i} \int_{\delta} f(q)q^{-n} dq / q\]

Where \(\delta\) is a small circle turning around \(q = 0 \in \mathbb{C}\) anticlockwise. This is

\[f_n = \int f(\tau)e^{-2\pi n\tau} d\tau = e^{2\pi n} \int_{0}^{1} f(x + iy)e^{-2\pi inx} dx \quad (2.36)\]

The function \(\left(f(\tau)(Im \tau)^{1/2}\right)\) is invariant under the action of \(SL(2, \mathbb{Z})\), and so, it gives us a function in \(SL(2, \mathbb{Z}) \setminus \mathbb{H}\). Since
\[ |f(\tau)| \sim O(q) \sim O(e^{-2\pi y}) \]

This function is bounded when \( y \to \infty \), and so, there exists a constant \( M \) such that
\[ |f(\tau)| \leq M y^{-\frac{1}{2}} \quad \forall \tau \in \mathbb{H} \]

Putting this in (2.36) we have
\[ |f_n| \leq e^{2\pi y} \cdot M \cdot y^{\frac{1}{2}} \]

Here, \( y \) can be any positive number, we put \( y = \frac{1}{n} \) and get the desired result. \( \blacksquare \)

As a corollary we get

**Proposition 2.15.1** Let \( f \) be a holomorphic modular form of weight \( k \) for \( SL(2, \mathbb{Z}) \). Then
\[ f_n = O(n^{k-1}) \]

**Proof.** Let \( \sigma_k \) be the Einstein series of weight \( k \), and \( \lambda \in \mathbb{C} \), be constant such that \( \lambda \sigma_k + f \) is a cusp form. The proposition follow from theorem 2.15.1 and the asymptotic behaviour of Fourier coefficients of \( \sigma_k \):
\[ \sigma_{k-1}(n) = \sum_{d|n} d^{k-1} = O(n^{k-1}) \]

Because
\[ \frac{\sigma_{k-1}(n)}{n^{k-1}} = \sum_{d|n} \left( \frac{d}{n} \right)^{k-1} \]
\[ = \sum_{d|n} \left( \frac{1}{d} \right)^{k-1} \leq \sum_{d=1}^{\infty} \frac{1}{d^{k-1}} = \xi(k-1) < \infty \]

Since \( n^{\frac{k}{2}} \) compared to \( n^{k-1} \) is negligible, we get the result. Deligne in [Deligne 1973] has shown that for a cusp form \( f \), we have
\[ f_n = O\left(n^{\frac{k}{2} - \frac{1}{2}} \sigma_0(n)\right) \] (2.37)

Where \( \sigma_0(n) \) is the number of positive divisors of \( n \). This implies that
\[ f_n = O\left(n^{\frac{k}{2} - \frac{1}{2} + \varepsilon}\right), \quad \forall \varepsilon > 0 \]

According to [Milne], Deligne in 1969 proved that (2.37) follows from the Weil conjectures for varieties over finite fields and he proved the Weil conjectures in 1973.
2.16 Dedekind eta function

According to [Apostol] the Dedekind eta function

$$\eta(\tau) := e^{\frac{2\pi i}{\tau}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau})$$

was introduced by Dedekind in 1877. We know that

$$\Delta(\tau) = (2\pi i)^{12} \eta^{24}$$

and the functional equation of $\Delta$ with respect to the action of $SL(2, \mathbb{Z})$. Taking 12th root of this we get

$$\eta \left( \frac{a\tau + b}{c\tau + d} \right) = \varepsilon(A) \left( -i(c\tau + d)^{\frac{1}{12}} \right) \eta(\tau)$$

for some $\varepsilon$ which is a 12th root of unity and depends only on $A$ and $\tau$. In fact

**Theorem 2.16.1** (Dedekind functional equation) We have

$$\eta \left( \frac{a\tau + b}{c\tau + d} \right) = \varepsilon(A) \left( -i(c\tau + d)^{\frac{1}{12}} \right) \eta(\tau)$$

For all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ with $c > 0$, where

$$\varepsilon(A) := \exp \left( \pi i \left( \frac{a + d}{2c} + S(d, c) \right) \right)$$

$$S(d, c) := \sum_{\gamma = 1}^{k-1} \frac{\gamma}{k} \left( \left\lfloor \frac{\gamma \cdot c}{r} \right\rfloor - \frac{1}{2} \right)$$

$$a := a - [a]$$

For a proof see [Apostol] Theorem 3.4. For $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ we get

$$\eta \left( \frac{-1}{\tau} \right) = (-i\tau)^{\frac{1}{2}} \eta(\tau)$$

2.17 Modular forms as k-fold differential

Let $f$ be a meromorphic function in $\mathbb{H}$. Show that the k-fold differential

$$f(\tau) d\tau \otimes d\tau \otimes \cdots \otimes d\tau \quad \text{k-times}$$
is invariant under $SL(2, \mathbb{Z})$, (and hence it induces a $k$-fold differential in $SL(2, \mathbb{Z}) \backslash \mathbb{H}$) if and only if $f$ is a meromorphic modular form of weight $2k$ for $SL(2, \mathbb{Z})$.

### 2.18 Petersson scalar product

We follow [Lang] page 37. Our main theorem in this section is that the space of cusps of weight $k$ for $SL(2, \mathbb{Z})$ has a basis of eigenforms. For this we have to put a Hermitian form on $S_k(SL(2, \mathbb{Z}))$. This will be the Petersson scalar product.

Let $\Gamma \subseteq SL(2, \mathbb{Z})$ be a subgroup of finite index and let $f, g$ be two holomorphic functions on $\mathbb{H}$. We define

$$\langle f, g \rangle := \frac{1}{[SL(2, \mathbb{Z}) : \Gamma]} \int_{\Gamma \backslash \mathbb{H}} f(\tau) \overline{g(\tau)} \frac{dx \wedge dy}{y^2}$$

where $\tau = x + iy$. In order to digest this definition we make the following comments:

1. We have

$$\frac{dx \wedge dy}{y^2} = \frac{i}{2} \frac{d\tau \wedge d\tau}{Im(\tau)}$$

and this is invariant under $GL^+(2, \mathbb{R})$ action. This follows from

$$d(A\tau) = (c\tau + d)^{-2} \det(A) \cdot d\tau$$

$$Im(A\tau) = Im(\tau) \cdot \det(A)|c\tau + d|^2$$

(2.38)

Let us define

$$f|_kA = f(A\tau)(c\tau + d)^{-k}(\det A)^{\frac{k}{2}}$$

$$\Omega(f, g) := f(\tau) \overline{g(\tau)} Im(\tau)^k \frac{i}{2} \frac{d\tau \wedge d\tau}{Im(\tau)^2}$$

We have

$$\Omega \left( f|_kA, g|_kA \right) = \Omega(f, g)(A\tau)$$

(2.39)

which follows from (2.38).

2. We will take $f, g$ two modular form of weight $k$ for a subgroup $\Gamma \subseteq SL(2, \mathbb{Z})$ of definite index. In this way for $A \in \Gamma$, $\Omega(f, g)$ is invariant under the action of $\Gamma$ and so it gives a differential form on $\Gamma \backslash \mathbb{H}$. The integration is over this space. The integration can be also taken over a fundamental domain of the action $\Gamma$ on $\mathbb{H}$.

3. The factor $[SL(2, \mathbb{Z}) : \Gamma]$ is inserted so that $\langle f, g \rangle$ becomes independent of the group $\Gamma$, that is if $f, g$ are modular forms of weight $k$ for $\Gamma_1 \subseteq \Gamma_2$ then $\langle f, g \rangle$ defined using the group $\Gamma_1$ is the same as $\langle f, g \rangle$ defined by the group $\Gamma_2$. For two groups $\Gamma_1, \Gamma_2$ we repeat this argument twice for $\Gamma_1 \cap \Gamma_2 \subseteq \Gamma_i, \ i = 1, 2$.

4. We have to check that the integral is convergent. For this we have to assume that $f, g$ are cusp forms. The fundamental domain for $\Gamma$ is a union of finite number
of translates (under $\Gamma$) of the classical fundamental domain $\hat{F}$ for $\text{SL}(2, \mathbb{Z})$

$$F = \bigcup_{A \in \Gamma \setminus \text{SL}(2, \mathbb{Z})} A\hat{F}$$

It is enough to show that the integral converges for $\text{Im}(\tau) \to +\infty$. For a cusp form $f$ we have

$$|f(\tau)| \ll c_1 e^{-c_2 \text{Im}(\tau)}$$

for sufficiently large $\text{Im}(\tau)$, and so, if one for $g$ is a cusp form, then the integral converges.

For $A \in \text{GL}^+(2, \mathbb{R})$ Let us define

$$A' := A^{-1} \cdot \det(A).$$

**Theorem 2.18.1** Let $f, g$ be cusp forms of weight $k$ for $\Gamma \subset \text{SL}(2, \mathbb{Z})$. Let also $A \in \text{GL}^+(2, \mathbb{Q})$. We have

1. $\langle f|A, g|A \rangle = \langle f, g \rangle$
2. $\langle f|A, g \rangle = \langle f, g|A' \rangle$
3. The scalar product in item 2 above above depends only on double cosets $\Gamma A \Gamma$

**Proof.**

$$\langle f|A, g|A \rangle = \frac{1}{[\text{SL}(2, \mathbb{Z}) : \Gamma]} \int_{\hat{F}} \Omega(f|A, g|A)$$

$$= n \int_{\hat{F}} \Omega(f, g)(A\tau) = n \int_{A\hat{F}} \Omega(f, g)$$

Here, $\hat{F}$ is a fundamental domain for $\Gamma$, and so $A\hat{F}$ is a fundamental domain for $A\Gamma A^{-1}$. We take smaller $\Gamma$ such that

$$A\Gamma A^{-1} \subseteq \text{SL}(2, \mathbb{Z})$$

For instance, we replace $\Gamma$ with $A^{-1} \text{SL}(2, \mathbb{Z}) A \cap \Gamma$. This has still finite index in $\text{SL}(2, \mathbb{Z})$. This gives us

$$[\text{SL}(2, \mathbb{Z}) : \Gamma] = [\text{SL}(2, \mathbb{Z}) : A\Gamma A^{-1}]$$

and the first part follows.

The second part follows from the first part and

$$g|A' = (g|A^{-1})$$

Note that $\det(A') = \det(A)$ and here we use the new definition of the slash operator.
Theorem 2.18.2  The Hecke operators acting on $S_k(SL(2, \mathbb{Z}))$ are Hermitian with respect to the Petersson scalar product that is

\[ \langle T_n f, g \rangle = \langle f, T_n g \rangle \]

Proof.  For $A \in \text{Mat}_n(2, \mathbb{Z})$ we have

\[ \langle f |_{kA}, g \rangle = \langle f, g |_{kA} \rangle \]

The map $SL(2, \mathbb{Z}) \rightarrow \text{Mat}_n(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}) \rightarrow \text{Mat}_n(2, \mathbb{Z})$

is a bijection

\[ \blacksquare \]

Proposition 2.18.1  The eigenvalues of $T'_n$'s are totally real algebraic numbers. The space of cusp form has a basis of eigenforms.

2.19 Computing $E_2$ as a double sum

In [Mov 12] we have considered the following family of elliptic curves

\[ y^2 = 4x^3 - t_2x - t_3 \]

\[ \alpha = \frac{dx}{y}, \quad \omega = (x + t_1) \frac{dx}{y} \]

\[ (t_1, t_2, t_3) = (a_1(\tau), a_2E_4(\tau), a_3E_6(\tau)) \]

We have $E \rightarrow \mathbb{C}/\mathbb{Z} + \mathbb{Z}$ and if $\delta_1, \delta_2$ are cycles in $E$ corresponding to vectors $\tau, 1$ then

\[ \begin{pmatrix} \int_{\delta_1} \frac{dx}{y} & \int_{\delta_1} (x + t_1) \frac{dx}{y} \\ \int_{\delta_2} \frac{dx}{y} & \int_{\delta_2} (x + t_1) \frac{dx}{y} \end{pmatrix} = \begin{pmatrix} \tau & -1 \\ 1 & 0 \end{pmatrix} \]

Let us consider the equality corresponding to $1, 2$ and $(2, 2)$ entries.

\[ t_1 \cdot \tau = -1 \int_{\delta_1} \frac{x dx}{y} = -1 - \int_0^\tau \phi(\tau, z) dz \quad (2.40) \]

\[ t_1 = - \int_{\delta_1} \frac{x dx}{y} = - \int_{0}^{\tau} \phi(\tau, z) dz \]

The integration in (2.41) can be replaced with integration over $\phi$ bellow:
Recall Weierstrass zeta function

\[ \xi(z) = \frac{1}{z} + \sum_{\omega \in \Lambda} \frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \]

It has the following properties

\[ \frac{d}{dz} \xi(z) = -\wp(z) \tag{2.42} \]

\[ \xi(z + \omega) - \xi(z) = 2\xi \left( \frac{1}{2} \omega \right), \quad \omega \notin 2\Lambda \tag{2.43} \]

see [Silvermann] page 40. We continue the computation of \( t_1 \)

\[ t_1 + \int_{\delta_1} d\xi(z) = xi(1 - \epsilon) - \xi(-\epsilon) = 2\xi \frac{1}{2} \]

and so

\[ a_1 E_2(\tau) = 4 + \sum_{d \mid (n,m) \neq (0,0)} \frac{4}{(1 - 2n\tau 2m)} + \frac{2}{(n\tau + m)} + \frac{1}{(n\tau + m)^2} \]

In a similar way

\[ t_1 \cdot \tau = -1 + 2\xi \left( \frac{\tau}{2} \right) \quad \text{(integration over } \delta_1) \]

\[ t_1 \cdot (\tau + 1) = -1 + 2\xi \left( \frac{\tau + 1}{2} \right) \quad \text{(integration over } \delta_1 + \delta_2) \]

**Problem 2.19.1** Write \( E_2 \) as a convergent power series on the generalized period domain.
Chapter 3
Elliptic curves and integrals

Although most of the seminars I couldn’t understand, after 10 times I started to get something and that something could be very useful for my development in mathematics or even to physics eventually, (S.-T. Yau in Kavli IPMU News No. 33 March 2016).

3.1 Introduction

In this chapter we study elliptic curves over complex numbers and the corresponding elliptic integrals.

3.2 Elliptic integrals

We start with an elliptic integral of the form

$$\int_{a}^{b} \frac{dx}{\sqrt{p(x)}}, \quad (3.1)$$

where \(p(x)\) is a polynomial of degree 3 and with three distinct real roots, and \(a, b\) are two consecutive elements among the roots of \(p\) and \(\pm \infty\). For instance, the polynomial \(p(x) := 4x^3 - t_2x - t_3, \quad t_2, t_3 \in \mathbb{C}\) has three distinct roots if and only if \(\Delta := 27t_3^2 - t_2^3 \neq 0\). If \(p(x)\) has repeated roots one can compute it easily.

Exercise 19 Compute the indefinite integral

$$\int \frac{dx}{\sqrt{p(x)}}, \quad (3.2)$$
where \( p \) is a polynomial of degree 1 and 2. Compute it also when \( p \) is of degree 3 but it has double roots. These integrals are computable because \( y^2 = P(x) \) is a rational curve! Let \( p \) be a polynomial of degree 3 and with three real roots \( t_1 < t_2 < t_3 \). Show that two of the four integrals

\[
\int_{-\infty}^{t_1} \frac{dx}{\sqrt{p(x)}}, \quad \int_{t_1}^{t_2} \frac{dx}{\sqrt{p(x)}}, \quad \int_{t_2}^{t_3} \frac{dx}{\sqrt{p(x)}}, \quad \int_{t_3}^{+\infty} \frac{dx}{\sqrt{p(x)}},
\]

can be computed in terms of the other two.

In many calculus books we find tables of integrals and there we never find a formula for elliptic integrals. Already in the 19th century, it was known that if we choose \( p \) randomly (in other words for generic \( p \)) such integrals cannot be calculated in terms of until then well-known functions. For particular examples of \( p \) we have some formulas calculating elliptic integrals in terms of the values of the Gamma function on rational numbers.

Exercise 20 For particular examples of polynomials \( p \) of degree 3, there are some formulas for elliptic integrals [3.2] in terms of the values of the Gamma function on rational numbers. For instance, verify the equality

\[
\int_{\gamma}^{+\infty} \frac{dx}{\sqrt{x^3 - 35x - 98}} = \frac{\Gamma\left(\frac{1}{4}\right) \Gamma\left(\frac{3}{4}\right) \Gamma\left(\frac{4}{4}\right)}{2\pi i \sqrt{-7}}.
\]  

(3.3)

In [Wal06] page 439 we find also the formulas

\[
\frac{\Gamma\left(\frac{1}{4}\right) \Gamma\left(\frac{3}{4}\right) \Gamma\left(\frac{4}{4}\right)}{2\pi i \sqrt{-7}}.
\]
3.2 Elliptic integrals

\[
\int_0^1 \frac{dx}{\sqrt{1-x^3}} = \frac{\Gamma\left(\frac{1}{3}\right)^2}{4\pi^{\frac{3}{2}}},
\]

\[
\int_0^1 \frac{dx}{\sqrt{x-x^3}} = \frac{\Gamma\left(\frac{1}{4}\right)^2}{2\pi^{\frac{3}{2}}},
\]

These formulas can be also derived using the software Mathematica. The Chowla-Selberg theorem, see for instance Gross’s articles [Gro78, Gro79], describes this phenomenon in a complete way. The right hand side of (3.3) can be written in terms of the Beta function which is more natural when one deals with the periods of algebraic differential forms.

The fact that we only need two of the integrals in (3.1) in order to calculate the others, can be easily seen by considering the integration in the complex domain \(x \in \mathbb{C}\), in which we may discard the assumption that \(p\) has only real roots. The integration is done over a path \(\gamma\) in the \(x \in \mathbb{C}\) domain which connects two points in the set of roots of \(p\) and \(\infty\), and avoids other roots except at its start and end points. An amazing fact that we learn in a complex analysis course is that if the path \(\gamma\) moves smoothly, without violating the properties as before, then the value of the integral does not change. This is certainly the origin of homotopy theory, or at least one of them. The next step in the study of elliptic integrals is the invention of the \(y\) variable which is basically the square root of \(p(x)\):

\[
E := \{(x,y) \in \mathbb{C}^2 \mid y^2 = p(x)\}.
\] (3.4)

This is called an elliptic curve in Weierstrass form.

**Theorem 3.2.1** The set \(E\) as a topological space is a compact torus minus one point, see Figure 3.1.

**Proof.**

We add another point \(O\) to \(E\) and will call it the point at infinity. We write \(\hat{E} = E \cup \{O\}\) and sometimes by abuse of notation use the same letter \(E\) for \(\hat{E}\). If we write the equation of \(E\) in homogeneous coordinates \([x:y:z] \in \mathbb{P}^2\) then

\[
O = [0:1:0],
\]

We define \(H_1(E, \mathbb{Z})\) as the abelization of the fundamental group of \(E\), that is, the quotient of the fundamental group of \(E\) by its subgroup generated by commutators:

\[
H_1(E, \mathbb{Z}) := \pi_1(E, b) / [\pi_1(E, b), \pi_1(E, b)],
\] (3.5)

where for a group \(G\), \([G,G]\) is the subgroup of \(G\) generated by the commutators \(aba^{-1}b^{-1}, a, b \in G\). It turns out that the integrals

\[
\int_{\delta} \omega, \delta \in H_1(E, \mathbb{Z}).
\]
are well-defined. The following Proposition can be proved without the help of Theorem 3.2.1.

**Proposition 3.2.1** The abelian group $H_1(E, \mathbb{Z})$ is free of rank 2, and hence, it is isomorphic to $(\mathbb{Z}^2, +)$.

**Proof (Sketch).** We prove that the non-abelian group $\pi_1(E, b)$ is free and it is generated by two elements. Let $\pi : E \to \mathbb{C}$ be the projection into $x$-coordinate and $a$ be the $x$-coordinate of $b$. The map $\pi$ is 2 to 1, except at $(t_1, 0), (t_2, 0), (t_3, 0)$, where $t_i$’s are the root of $p(x)$. An element $\delta$ of the homotopy group $\pi_1(E, b)$ can be identified with $\delta := \pi(\gamma) \in \pi_1(\mathbb{C} \setminus \{t_1, t_2, t_3\}, a)$ which has this property that the multivalued function $y := \sqrt{p(x)}$ along $\gamma$ is one valued. The closed paths $\gamma_1$ and $\gamma_2$ in Figure 3.1 are in the image of $\pi$, let us say $\pi(\delta_i) = \gamma_i, \ i = 1, 2$, and $\delta_1, \delta_2$ generate $\pi_1(E, b)$ freely. \qed

Another important ingredient of $H_1(E, \mathbb{Z})$ is the skew symmetric intersection bilinear map

$$H_1(E, \mathbb{Z}) \times H_1(E, \mathbb{Z}) \to \mathbb{Z}$$

The cycles $\delta_1$ and $\delta_2$ can be chosen in such a way that $\langle \delta_1, \delta_2 \rangle = -1$.

**Proposition 3.2.2** Let $\delta_1$ and $\delta_2$ be generators of $H_1(E, \mathbb{Z})$ with $\langle \delta_1, \delta_2 \rangle = -1$. Then the quotient

$$\tau := \frac{\int_{\delta_1} \frac{dx}{y}}{\int_{\delta_2} \frac{dx}{y}}$$

has positive imaginary part.

**Proof (sketch).** First we note that $\omega := \frac{dx}{y}$ restricted to $E$ is holomorphic even at the infinity point $O$. The statement follows from

$$\sqrt{-1} \left( \int_{\delta_1} \omega \int_{\delta_2} \omega - \int_{\delta_2} \omega \int_{\delta_1} \omega \right) = \sqrt{-1} \int_E \omega \wedge \bar{\omega} > 0,$$

where $\omega = \frac{dx}{y}$. The equality follows from Stokes theorem for the complement of $\delta_1$ and $\delta_2$ in $E$. In local holomorphic coordinate system $z = x_1 + \sqrt{-1} x_2$ in $E$ we have $\omega = f(z)dz, \ f(z)$ holomorphic, and

$$\omega \wedge \bar{\omega} = |f(z)|^2dz \wedge d\bar{z} = -\sqrt{-1} |f(z)|^2dx_1 \wedge dx_2.$$

\qed

**Definition 3.2.1** The lattice of elliptic integrals is

$$\int_{H_1(E, \mathbb{Z})} \frac{dx}{y} = \mathbb{Z} \int_{\delta_1} \frac{dx}{y} + \mathbb{Z} \int_{\delta_2} \omega,$$

where $\delta_1, \delta_2$ is a basis of $H_1(E, \mathbb{Z})$ with $\langle \delta_1, \delta_2 \rangle = -1$. 
3.3 Elliptic curves in Weierstrass format

We consider again the family of elliptic curves

\[ E_t = E_{t_2, t_3} = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - t_2x - t_3\}, \quad t \in T \] (3.6)

\[ T := \mathbb{C}^2 - \{(t_2, t_3) \in \mathbb{C}^2 \mid \Delta = 0\}, \quad \Delta := t_2^3 - 27t_3^2. \] (3.7)

The curve \( E_t \) is called an elliptic curve in the Weierstrass format.

3.4 Picard-Lefschetz theory

By Ehresmann’s theorem the fibration \( E_t, t \in T \) is a \( C^\infty \) bundle over \( T \), i.e. it is locally trivial. This is the basic stone for the Picard-Lefschetz theory (see for instance [Mov04] and the references there). It gives us the following linear action:

\[ \pi_1(T, b) \times H_1(E_b, \mathbb{Z}) \to H_1(E_b, \mathbb{Z}) \]

where \( b \in T \) is a fixed point. In order to calculate it we proceed as follows: First we choose two cycles \( \delta_1, \delta_2 \in H_1(E_b, \mathbb{Z}) \). For the fixed parameter \( t_2 \neq 0 \), define the function \( f \) in the following way:

\[ f: \mathbb{C}^2 \to \mathbb{C}, \quad (x, y) \mapsto -y^2 + 4x^3 - t_2x. \]

The function \( f \) has two critical values given by \( \tilde{t}_3, \tilde{t}_3 = \pm \sqrt{t_2/27} \). In a regular fiber \( E_{\tilde{t}_3} = f^{-1}(\tilde{t}_3) \) of \( f \) one can take two cycles \( \delta_1, \delta_2 \) such that \( \langle \delta_1, \delta_2 \rangle = 1 \) and \( \delta_1 \) (resp. \( \delta_2 \)) vanishes along a straight line connecting \( t_3 \) to \( \tilde{t}_3 \) (resp. \( \tilde{t}_3 \)). The corresponding anti-clockwise monodromy around the critical value \( \tilde{t}_3 \) (resp \( \tilde{t}_3 \)) can be computed using the Picard-Lefschetz formula:

\[ \delta_1 \mapsto \delta_1, \quad \delta_2 \mapsto \delta_2 + \delta_1 \quad (\text{resp. } \delta_1 \mapsto \delta_1 - \delta_2, \quad \delta_2 \mapsto \delta_2). \]

It is not hard to see that the canonical map \( \pi_1(\mathbb{C} \setminus \{\tilde{t}_3, \tilde{t}_3\}, b) \to \pi_1(T, t) \) induced by inclusion is an isomorphism of groups and so the image of the monodromy group written in the basis \( \delta_1 \) and \( \delta_2 \) is:

\[ \langle A_1, A_2 \rangle = \text{SL}(2, \mathbb{Z}), \quad \text{where } A_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}. \]

Note that \( g_1 := A_2^{-1}A_1^{-1}A_2^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad g_2 := A_1^{-1}A_2^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \) and \( \text{SL}(2, \mathbb{Z}) = \langle g_1, g_2 \mid g_1^2 = g_2^2 = -I \rangle \), where \( I \) is the identity \( 2 \times 2 \) matrix.

**Exercise 21** Discuss the Picard-Lefschetz theory as above for the Legendre family of elliptic curves:
\( y^2 = x(x - 1)(x - \lambda) \)

### 3.5 Weierstrass uniformization theorem

Let

\[
t := (g_2, g_3) = (60G_4(\Lambda), 140G_6(\Lambda)),
\]

where \( G_4 \) and \( G_6 \) are complex numbers defined in (2.10). From Proposition 2.14.1 it follows that \( g_3^2 - 27g_2^3 \neq 0 \) and so \( t \in \mathbb{T} \), where \( \mathbb{T} \) defined in (3.7) (do not use the product formula for the discriminant in (2.33)). Let \( E_t \) be the corresponding elliptic curve in (3.6). From the differential equation of the Weierstrass \( \wp \) function, see Theorem 2.5.1, it follows that we have a map

\[
f : \mathbb{C}/\Lambda \longrightarrow E_t,
\]

\[
z \longmapsto (\wp(\Lambda, z), \wp'(\Lambda, z)), \quad f(0) = O.
\]

(3.8)

**Theorem 3.5.1** *The map (3.8) is an isomorphism of sets.*

Actually, \( f \) is an isomorphism of Riemann surfaces. Moreover, we will see that \( E_t \) has a structure of a group and it is also a morphism of groups.

**Proof.** The heart of the proof is Theorem 2.4.1. Let \((x, y) \in E_t\). The elliptic function \( \wp(z) - x \) has a pole of order two at \( z = 0 \). Therefore, it must have two zeros \( z_1, z_2 \) in \( \mathbb{C}\setminus\Lambda \). By the differential equation of \( \wp \), we know that \( \{\wp'(z_1), \wp'(z_2)\} = \{y, -y\} \).

If \( y \neq 0 \) then there is exactly one of \( z_i \)'s, let us say \( z_1 \), such that \( \wp'(z_1) = y \). If \( y = 0 \) then \( \wp \) has a zero of multiplicity 2 at \( z_1 \) and hence \( z_1 = z_2 \) in \( \mathbb{C}/\Lambda \). This argument proves that \( f \) is one to one and surjective. \( \square \)

Let \( \delta_1 \) and \( \delta_2 \) be closed paths in \( \mathbb{C}/\Lambda \) which are the images of the vectors \( \omega_1, \omega_2 \in \mathbb{C} \) under the canonical map \( \mathbb{C} \rightarrow \mathbb{C}/\Lambda \). We also use the same notation for their images in \( E_t \) under the map (3.8).

We have

\[
\int_{\delta_i} \frac{dx}{y} = \omega_i, \quad i = 1, 2.
\]

(3.9)

In particular, the lattice of elliptic integrals for \( E_t \) as above is \( \Lambda \). The inverse of \( f \) in (3.8) can be given explicitly as follows:

\[
f^{-1} : E_t \rightarrow \mathbb{C}/\Lambda
\]

\[
f^{-1}(P) := \int_P \frac{dx}{y}
\]

(3.10)

The integration can be interpreted in the following way. We take a path in the \( x \)-plane which connects the infinity to the \( x \)-coordinate of \( P \). We also choose a branch of \( \frac{dx}{y} = \frac{dx}{\sqrt{P(x)}} \). In geometric terms, this is to say, we connect \( P \) to the point at infinity.
3.6 Sketch of the proof of Theorem (2.9.1)

Let $P$ be the space of lattices.

**Theorem 3.5.2** The map given by

$$p : \mathbb{C}^2 \setminus \{t_2^3 - 27t_3^2 = 0\} \to \mathcal{P}$$

$$(t_2, t_3) \mapsto \int_{\mathbb{H}_1(t_2, t_3)} \frac{dx}{y}$$

is well-defined and it is a biholomorphism which satisfies

$$p(t_2 \lambda^{-4}, t_3 \lambda^{-6}) = \lambda p(t_2, t_3), \quad \lambda \in \mathbb{C}, \; \lambda \neq 0.$$ 

*Its inverse $p^{-1}$ is given by the Eisenstein series:*

$$\Lambda \to (g_2(\Lambda), g_3(\Lambda)) = (60G_4, 140G_6)$$

**Proof.** The fact that $p$ is well-defined follows from Theorem 3.2.2. From Theorem 3.8 we can easily derive $p \circ p^{-1} = Id$ which implies that $p^{-1}$ is injective. The equality $p^{-1} \circ p = Id$ is equivalent to the fact that $p$ is injective. This in turn is equivalent to the injectivity of $j : \text{SL}(2, \mathbb{Z}) \setminus \mathbb{H} \to \mathbb{C}.$ [Proof of this fact!!!!]

**Exercise 22** Ex. 6.2, 6.4, 6.6, 6.7, 6.14 of [Sil92].

### 3.6 Sketch of the proof of Theorem (2.9.1)

We regard modular forms as functions on the space of lattices $\mathcal{P}$. Under the bijection $p$ any modular form of weight $y$ becomes a holomorphic function $f$ in $T$ with the property

$$f(t_2 \lambda^{-4}, t_3 \lambda^{-6}) = \lambda^k f(t_2, t_3) \quad (3.11)$$

We use the growth condition of $f$ and prove that $f$ is a polynomial of degree $k$ in the weighted ring

$$\mathbb{C}[t_2, t_3], \; \text{weight } (t_2) = 4, \; \text{weight } (t_3) = 6.$$ 

Since the lattices associated to $\tau$ and $\tau + 1$ are the same, we get a map $D - \{0\} \to \mathcal{P}$, where $D$ is the disc of radius 1 and center 0 in $\mathbb{C}$. We compose it with $p^{-1}$ and get the map
\[ i : D \rightarrow \mathbb{C}^2, \quad q \mapsto (g_2(q), g_3(q)) \]

Note that this map is even defined at 0 \( \in D \) and the image of 0 is in the discriminant locus \( \{ \Delta = 0 \} \). The growth condition of \( f \) implies that \( f |_{Im(i)} \) extends as a holomorphic function at \( i(0) \). Now, the \( \mathbb{C}^* \)-action in \( \mathbb{C}^2 \) implies that \( f \) extends to a holomorphic function in \( \mathbb{C}^2 \setminus \{(0,0)\} \). By Hartogs theorem we conclude that \( f \) is holomorphic in \( \mathbb{C}^2 \). We write the Taylor series of \( f \) at \( (0,0) \) and (3.11) implies the des

### 3.7 Some identities

Let \( E_t, \ t = (t_2, t_3) \) be an elliptic curve in Weierstrass format and let \( P = (x(P), y(P)) \) be a point of \( E_t \). In Theorem 3.5.1 in order to prove \( f \circ f^{-1} = Id \), we need to prove that:

\[
x(P) = \left( \frac{\int_0^P dx}{y} \right)^{-2} + \sum \left( \left( \int_0^P \frac{dx}{y} \right)^{-2} - \left( \int_0^P \frac{dx}{y} - \frac{\int_0^P \tilde{dx}}{y} \right)^{-2} \right) \]

\[
y(P) = (-2) \sum \left( \int_0^P \frac{dx}{y} \right)^{-3}
\]

where the sum is taken over all, except one, non-homotopic paths in \( E \) wich connect \( O \) to \( P \) and \( \int_0^P \) means integration over this path. In the above formulas the integration
over the exceptional path is denoted by $\hat{\int}_P$. It is easy to see that this doesn’t depend on the choice of exceptional path.

The Eisenstein series can be written in the following way. Let $\delta_0 \in H_1(E, \mathbb{Z})$ be a primitive element, that is, it is not divisable by an integer. We have

$$\zeta(k) \cdot \sum_{\delta \text{ a monodromy of } \delta_0} \left( \int_\delta \omega \right)^{-k} = G_k(E, \omega), \ k \geq 4, \ k \text{ even} \quad (3.12)$$

where the sum runs in all monodromies $\delta \in H_1(E, \omega)$ of $\delta_0$. Since the monodromy group of the Weierstrass family is $\text{SL}(2, \mathbb{Z})$, we can also take the sum over all primitive elements of $H_1(E, \mathbb{Z})$. The sums

$$\sum_{\delta \text{ a monodromy of } \delta_0, \ \langle \delta, \delta_0 \rangle > 0} \left( \int_\delta \omega \right)^{-k}, \ k \geq 3 \quad (3.13)$$

are related to the discussion after Theorem 2.7.1. These functions seem to give an embedding of the universal cover of $\mathbb{C}^2 \setminus \{27t_2^3 - t_3^2 = 0\}$ inside some affine space. The following sum might be also interesting:

$$\sum_{\delta \text{ a clockwise monodromy of } \delta_0} \left( \int_\delta \omega \right)^{-k} \quad (3.14)$$

### 3.8 Schwarz function

Let us take the Legendre family of elliptic curves and consider the Schwarz function

$$\lambda \mapsto \frac{\int_{\delta_1} \frac{dz}{\lambda}}{\int_{\delta_2} \frac{dz}{\lambda}} \in \mathbb{H}$$

It is multivalued because of the choice of $\delta_1, \delta_2$. In order to get a one valued function we restrict $\lambda$ to $\mathbb{H}$ and choose cycles $\delta_i, \ i = 1, 2$ such that the projection of $\delta_i$ (resp. $\delta_2$) to the $x$-plane is a cycle around 0 (resp. 1) and $\lambda$. In this way the Schwarz function is a biholomorphism. Its analytic continuations around $\lambda = 0, 1$ corresponds to the Picard-Lefschetz transformation of $\delta_1$ and $\delta_2$.

**Exercise 23** Show that the image of the Schwarz function is the region depicted in $\mathbb{H}$. The analytic continuations of the Schwarz map gives us the triangulation of $\mathbb{H}$. 

\[1\] Reproduced from Wikipedia
3.9 CM elliptic curves

Recall that $\mathcal{P}$ is a complex manifold whose points are lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. In fact one can reinterpret it as follows:

**Exercise 24** $\mathcal{P}$ is the moduli of triples $(E, \omega, p)$, where $E$ is a Riemann surface of genus one, $p \in E$, and $\omega$ is a holomorphic differential form on $E$. The canonical action of $a \in \mathbb{C}^*$ on $\mathcal{P}$ corresponds to the multiplication of $\omega$ with $a^{-1}$.

**Definition 3.9.1** The endomorphism group of an elliptic curve $E = E_\Lambda$ is the set of all holomorphic maps $E_\Lambda \to E_\Lambda$ which are in addition homomorphisms of groups. It is in one to one correspondance with

$$\text{End}(E) = \{ \alpha \in \mathbb{C} \mid \alpha \Lambda \subset \Lambda \}$$

We have $\mathbb{Z} \subset \text{End}(E)$ and we say that $E$ is CM if the inclusion is strict.

Later, we will encounter two special CM elliptic curves as follows:

**Exercise 25** Classify all elliptic curves $E$ with $\alpha \in \text{End}(E)$ which is not multiplication by $\pm 1$ and is an isomorphism. More precisely show that we have only two such elliptic curve

$$E = E_{\langle z, 1 \rangle}, \ z = i, \frac{-1 + i\sqrt{3}}{2}.$$

**Exercise 26** Ex. 8,9,10,12 of Koblitz.

3.10 Fourier expansions and elliptic integrals

Let $E_z, z \in \mathbb{P}'$ be a family of elliptic curves with a singular fiber at $z = 0$. Further, assume that the monodromy

$$H_1(E_z, \mathbb{Z}) \to H_1(E_z, \mathbb{Z})$$

For $z$ near 0 and in a basis $\delta_1, \delta_2 \in H_1(E, \mathbb{Z}), \langle \delta_1, \delta_2 \rangle = -1$ is given by
\[
\begin{pmatrix}
\delta_1 \\
\delta_2
\end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix}
\delta_1 \\
\delta_2
\end{pmatrix}
\]

Moreover, for a holomorphic differential form
\[
I_2 : = \int_{\delta_z} \omega = \text{holomorphic at } z = 0 \text{ and } I_2(0) \neq 0
\]
\[
I_1 = \frac{\ln z + \tilde{I}_1}{2\pi i}
\]
\[
\tilde{I}_1 = \text{holomorphic at } z = 0 \text{ and } \tilde{I}_1(0) \neq 0
\]

For an explicit example see [Movasati 2012]. The mirror map is defined in the following way
\[
\tau = \frac{I_1}{I_2} = \frac{1}{2\pi i} \left( \ln z + \tilde{I}_1 \right)
\]

For \( z \) near to \( O \) and taking the branch of \( \ln z \) with \( 0 < \text{Im}(\ln z) < 2\pi \), \( \tau \) is near \( i\infty \) and it is in the band
\[
\{ \tau \in \mathbb{C} | 0 \leq \text{Re}(\tau) \leq 1, \quad \text{Im}(\tau) > 0 \}
\]

For a modular form \( f \) we use (3.15) and we get
\[
f_n = \int_{\gamma} f \left( \frac{I_1(z)}{I_2(z)} \right) e^{-2\pi i \frac{I_1(z)}{I_2(z)}} d \left( \frac{I_1}{I_2} (z) \right)
\]
\[
= \int_{\gamma} f \left( \frac{I_1}{I_2} \right) - \sum_{m=0}^{\infty} \frac{Z^{-n}}{m!} \left( -\frac{I_1}{I_2} \right)^m \frac{I_2 \theta I_1 - I_1 \cdot \theta I_2}{I_2^2} \frac{dZ}{Z}
\]
\[
= \sum_{m=0}^{\infty} \frac{(-n)^m}{m!} \text{Residue} \left( gn(m(z), z = 0) \right), \quad (3.15)
\]

\[
\text{Residue} \left( gn(m(z), z = 0) \right) = f \left( \frac{I_1}{I_2} \right) \frac{I_2 \cdot \theta I_1 - I_1 \cdot \theta I_2}{I_2^2} \left( \frac{\tilde{I}_1}{I_2} \right)^m Z^{-n}
\]

In many concrete examples, \( f \left( \frac{I_1}{I_2} \right) \) turns out to be a rational function in \( I_2, \theta I_2, Z \).

More over, for large \( m, gn(m(z) \) turns out to to be holomorphic at \( z \) and so the sum in (3.15) is a actually finite.
Chapter 4
Rudiments of Algebraic Geometry of curves

Throughout the present text we work with a field $k$ of arbitrary characteristic and not necessarily algebraically closed. By $\overline{k}$ we mean the algebraic closure of $k$. The main examples that we have in mind are $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and a number field. A number field $k$ is a field that contains $\mathbb{Q}$ and has finite dimension, when considered as a vector space over $\mathbb{Q}$. A function field $\tilde{k}(t) = \tilde{k}(t_1, t_2, \ldots, t_s)$ over a field $\tilde{k}$ is the field of rational functions $\frac{a(t_1, t_2, \ldots, t_s)}{b(t_1, t_2, \ldots, t_s)}$, where $a$ and $b$ are polynomials in indeterminates $t_1, t_2, \ldots, t_s$ and with coefficients in $\tilde{k}$. Later, we will also use the field of $p$-adic numbers.

4.1 Curves

Let $k$ be a field and $k[x, y]$ be the space of polynomial in two variables $x, y$ and with coefficients in $k$. The $n$ dimensional affine space over $k$ is by definition

$$\mathbb{A}^n(k) = k \times k \times \cdots \times k,$$

$n$ times

and the projective $n$ dimensional space is

$$\mathbb{P}^n(k) := \mathbb{A}^{n+1}(k) - \{(0, 0, \cdots, 0)\} / \sim$$

$a \sim b$ if and only if $\exists \lambda \in k, a = \lambda b$

We will consider the following inclusion

$$\mathbb{A}^n(k) \to \mathbb{P}^n(k), \ (x_1, x_2, \cdots, x_n) \mapsto [x_1; x_2; \cdots; x_n; 1]$$
and call $\mathbb{P}^n$ the compactification of $\mathbb{A}^n$. The projective space at infinity is defined to be
$$\mathbb{P}^n_{\infty}(k) = \mathbb{P}^n(k) - \mathbb{A}^n(k) = \{ [x_1:x_2: \cdots : x_n:x_{n+1}] \mid x_{n+1} = 0 \}.$$ 

For simplicity, in the case $n = 1, 2$ and 3 we use $x, (x,y)$ and $(x,y,z)$ instead of $x_1, x_2, \ldots$.

Any polynomial $f \in k[x,y]$ defines an affine curve
$$C(k) := \{ (x,y) \in k^2 \mid f(x,y) = 0 \}.$$ 

The most famous Diophantine curve is given by $f = x^n + y^n - 1$. We denote it by $F_n$.

**Remark 4.1.1** The set $C(k)$ may be empty, for instance take $k = \mathbb{Q}$, $f = x^2 + y^2 + 1$.

This means that the identification of a curve with its points in some field is not a good treatment of curves. One of the starting points of the theory of schemes is this simple observation.

For $f \in k[x,y]$ we define the homogenization of $f$
$$F(x,y,z) = \epsilon^d f(\frac{x}{z}, \frac{y}{z}), \quad d := \deg(f).$$

$F$ defines a projective plane curve in $\mathbb{P}^2(k)$:
$$\tilde{C}(k) := \{ [x:y:z] \in \mathbb{P}^2(k) \mid F(x,y,z) = 0 \}.$$ 

Note that
$$\forall c \in k, (x,y,z) \in k^3, \quad F(cx, cy, cz) = \epsilon^d F(x,y,z).$$

One has the injection
$$C(k) \to \tilde{C}(k), \quad (x,y) \mapsto [x:y:1]$$

and for this reason one sometimes says that $\tilde{C}(k)$ is the compactification of $C(k)$.

Let $g$ be the last homogeneous piece of the polynomial $f$. By definition it is a homogeneous polynomial of degree $d$. The points in
$$\tilde{C}(k) - C(k) = \{ [x;y] \in \mathbb{P}^1 \mid g(x,y) = 0 \}$$

are called the points at infinity of $C(k)$. The set of points at infinity of $F_n$ is empty if $n$ is even and it is $\{(1;-1)\}$ if $n$ is odd.

**4.2 Charts**

From now on we use the notation $C$ to denote the curve $\tilde{C}$ in the previous section. We simply say that the curve $C$ in an affine chart is given by $f(x,y) = 0$. The projective space $\mathbb{P}^2$ is covered by three canonical charts:
$$\alpha : \mathbb{A}^2(k) \leftrightarrow \mathbb{P}^2(k)$$
$\alpha_1(x, y) = [x; y; 1], \ \alpha_2(x, z) = [x; 1; z], \ \alpha_3(y, z) = [1; y; z].$

and the curve in each chart is respectively given by

$f_1(x, y) := F(x, y, 1) = 0, \ f_2 := F(x, 1, z) = 0, \ \text{and} \ f_3 := F(1, y, z) = 0.$

We are also going to use the notion of an arbitrary curve over $k$ from algebraic geometry of schemes. Roughly speaking, a curve $C$ over $k$ means $C$ over $\bar{k}$ and the ingredient polynomials of $C$ are defined over $k$. The reader who is not familiar with those general objects may follow the text for affine and projective curves as above. The set $C(k)$ is now the set of $k$-rational points of $C$.

### 4.3 Schemes

We defined $\mathbb{P}^2(k)$ and $C(k)$ without defining $\mathbb{A}^2$ and $\mathbb{C}$. In this section we fill this gap and we explain the rough idea behind the definition of the schemes $\mathbb{P}^2$ and $C$.

By the affine scheme $\mathbb{A}^2$ we simply think of the ring $k[x, y]$. Open subsets of $\mathbb{A}^2$ are given by the localization of $k[x, y]$. We will need two open subsets of $\mathbb{A}^2$ given respectively by

$k[x, y, \frac{1}{x}]$ and $k[x, y, \frac{1}{y}]$

By the projective scheme $\mathbb{P}^2$ we mean three copies of $\mathbb{A}^2$, namely

$k[x, y], k[x, z], k[y, z]$

together with the isomorphism of affine subsets:

$k[x, y, \frac{1}{y}] \cong k[x, z, \frac{1}{z}], \ x \mapsto \frac{x}{z}, \ y \mapsto \frac{1}{z}$ \hspace{1cm} (4.1)

$k[x, y, \frac{1}{x}] \cong k[y, z, \frac{1}{y}], \ x \mapsto \frac{1}{z}, \ y \mapsto \frac{y}{z}$

$k[x, z, \frac{1}{x}] \cong k[y, z, \frac{1}{y}], \ x \mapsto \frac{1}{y}, \ z \mapsto \frac{z}{y}$

The best way to see these isomorphism is, for instance: we look at an element of $k[x, y]$ as a function on the first chart $\mathbb{A}^2(k)$ and for $(a, b)$ in this chart we use the identities

$[a; b; 1] = [\frac{a}{b}; 1; \frac{1}{b}] = [1; \frac{b}{a}; \frac{1}{a}]$.

We think of the the scheme $C$ in the same way as $\mathbb{P}^2$, but replacing $k[x, y]$ with $k[x, y]/\langle f_1 \rangle$ and so on. Here $\langle f_1 \rangle$ is the ideal $k[x, y]$ generated by a single element $f_1$. We can also think of $C$ in the same way as $\mathbb{P}^2$ but with the following additional relations between variables:
\[ f_1(x, y) = 0 \text{ in } k[x, y] \]
\[ f_2(x, z) = 0 \text{ in } k[x, z] \]
and
\[ f_3(y, z) = 0 \text{ in } k[y, z]. \]

**Remark 4.3.1** The above discussion does not use the fact that \( k \) is a field. In fact, we can use an arbitrary ring \( R \) instead of \( k \). In this way, we say that we have a scheme \( C \) over the ring \( R \).

The function field of the projective space \( \mathbb{P}^2 \) is defined to be
\[ k(\mathbb{P}^2) := k(x, y) \cong k(x, z) \cong k(y, z), \]
where the isomorphisms are given by (4.1). The field of rational function on the curve \( C \) is the field of fractions of the ring \( k[x, y]/\langle f_1 \rangle \). Using the isomorphism (4.1), this definition does not depend on the chart with \((x, y)\) coordinates. We can also think of \( k(C) \) as \( k(x, y) \) but with the relation \( f_1(x, y) = 0 \) between the variables \( x, y \). Any \( f \in k(C) \) induces a map
\[ C(k) \to k \]
that we denote it by the same letter \( f \).

**4.4 Singular and smooth curves**

**Definition 4.4.1** We say that an affine curve given by \( f(x, y) = 0 \) is singular if there is a point \((a, b) \in \bar{k}^2\) such that
\[ f(a, b) = f_x(a, b) = f_y(a, b) = 0. \]
where \( f_x \) is the derivation of \( f \) with respect to \( x \) and so on. The point \((a, b)\) is called a singularity of the affine curve. A projective curve is singular if one of its affine charts is singular. For a curve \( C \), affine or projective, we denote by \( \text{Sing}(C) \subset C(\bar{k}) \) the set of singular points of \( C \).

**4.5 Resultant and discriminant**

Let \( f, g \in \mathbb{Z}[x] \). In the order to compute the resultant of \( f, g \) we proceed as follows. We take one of \( f \) and \( g \), let us say \( f \), and define
\[ V := \mathbb{Q}[x]/f(x)\mathbb{Q}[x] \]
4.6 Discriminant

This is a vector space of dimension \( \deg(f) \) and it has the basis

\[
1, \ x, \ x^2, \ldots, x^{\deg(f) - 1}
\]  

(4.2)

Now consider the linear map

\[
A : V \rightarrow V \\
A(P(x)) := P(x) \cdot g(x)
\]

We write this map in the basis 4.2 and compute its characteristic polynomial

\[ F(s) := \det(A - sI) \]

It might be better from computational point of view to find the minimal polynomial

\[ F(s) \]

of \( A \), that is, a polynomial of minimal degree and with coefficients in \( Q \) such that

\[ F(A) = 0 \]

It follows that

\[ F(g(x)) = P(x) \cdot f(x) \]

for some polynomial \( P(x) \in Q[x] \). We have

\[
P(x) \cdot f(x) + Q(x) \cdot g(x) = F(0)
\]

(4.3)

where \( Q(x) = \frac{F(0) - F(g(x))}{g(x)} \in Q[x]\).

After multiplying 4.3 with a natural number we get an equality

\[
P(x) \cdot f(x) + Q(x) \cdot g(x) = \Delta
\]

where \( \Delta \in \mathbb{Z} \), \( P, Q \in \mathbb{Z}[x] \). We call \( \Delta \) the resultant of \( f, g \). The resultant of \( f(x), f'(x) \) is called the discriminant of \( f \).

4.6 Discriminant

Let \( R \) be a ring and \( k \) be the field of fractions of \( k \).

**Definition 4.6.1** Let us be given a polynomial \( f \in R[x, y, \ldots] \), where \( (x, y, \ldots) \) is a multi variable. The discriminant ideal of \( f \) contains all element \( \Delta \in R \) such that

\[
\Delta = f a_1 + f_2 a_2 + f_3 a_3 + \ldots, \quad \text{for some} \ a_1, a_2, \ldots \in R[x, y, \ldots].
\]

When the discriminant ideal is principal we denote by \( \Delta \) its generator and we call it the discriminant of the polynomial \( f \). It is defined up to units of the ring \( R \), and
hence in the case $R = \mathbb{Z}$ it is defined up to sign. In this case we fix this ambiguity by assuming that $\Delta$ is positive.

**Exercise 27** For

$$f = y^2 - x^3 - t_4 x - t_6, \quad t_4, t_6 \in \mathbb{R};$$

show that the discriminant ideal is generated by

$$\Delta = 2(4t_4^3 + 27t_6^2).$$

The corresponding $a_1, a_2$ and $a_3$ in this case are given by

$$a_1 = 2(27x^3 - 27y^2 + (27t_4)x + (-27t_6)),$n

$$a_2 = 2(-9x^4 + (-15t_4)x^2 + (-4t_4^2)), \quad a_3 = -54x^3y + 27y^3 + (-54t_4)xy.$$

In this case, $\Delta$ is the resultant of the polynomials $P(x)$ and $P_*(x)$, where $P = x^3 + t_4 x + t_6$.

In all the case below, the discriminant ideal is principal and we have calculated its generator.

$$f = y^2 - x^3 - t_4 x - t_6 - t_2 x^2 + t_1 xy + t_3 y.$$  

(4.5)

This modulo 2 is:

$$\Delta = t_1^4 t_2 t_3 + t_1^3 t_3 t_4 + t_1^6 t_6 + t_1^3 t_4 + t_1^4 t_2^2 + t_3$$

$$a_1 = t_1^6, \quad a_2 = t_1^4 x^2 + t_1^3 y + t_1^4 t_4$$

$$a_3 = t_1^3 x^3 + t_1^3 y + t_1^2 t_2 x + t_1^4 t_3 x + t_1^2 t_2 t_3 + t_1^4 t_4 + t_1^2 t_3^2 + t_1 t_3 x + t_3$$

For the case

$$f = y^2 - x^3 - t_4 x - t_6 - t_2 x^2.$$  

(4.6)

we have

$$\Delta = 2(4t_3^3 t_6 - t_2^2 t_6^2 - 18 t_2 t_4 t_6 + 4t_4^3 + 27t_6^2);$$
4.8 Discriminant of projective curves

\[ a_1 = 2(27t^3 - 27t^2 + (27t^2)x^2 + (27t^4)x + (-4t^3 + 18t^2 + 27t^6)); \]
\[ a_2 = 2(-9x^4 + (-12t^2)x^3 + (-t^2 - 15t^4)x^2 + (2t^3 - 10t^2 + t^2 + 4t^3 - 4t^3)); \]
\[ a_3 = -54x^3y + 27y^3 + (-54t^2)x^2y + (-54t^2)xy + (4t^3 - 18t^2)y; \]

Modulo 3 this is:
\[ \Delta = t_7^3 - t_2^6 - t_4^3 \]
\[ a_1 = t_2^3, \ a_2 = t_2^5x^2 + t_2^3x + t_2^6x - t_2^7 + t_4^3, \ a_3 = t_2^3. \]

4.7 The main property of the discriminant

The main property of the singular ideal is

**Proposition 4.7.1** Let \( I \) be any maximal ideal of \( R \) and so \( R/I \) is a field. The affine variety \( f = 0 \) is singular over \( R/I \) if and only if the discriminant ideal is a subset of \( I \).

Let us describe our main examples for the above theorem.

1. \( R = k \) and so \( I = \{0\} \).
2. \( R = \mathbb{Z} \). This is a principal ideal domain and so the discriminant ideal is generated by some \( \Delta \in \mathbb{N} \) and \( I \) is generated by some prime \( p \in \mathbb{N} \). In this case, \( f = 0 \) is singular over \( \mathbb{F}_p \) if and only if \( p \mid \Delta \).
3. \( R = k[t] \) and for \( a \in k \), \( I \) is the ideal of \( R \) generate by \( t_i - a_i \), \( i = 1, 2, \ldots, s \).

Let also assume that the discriminant ideal is generated by \( \Delta \). In this case, the curve \( f = 0 \) with the evaluation of the parameters \( t = a \) is singular if and only if \( \Delta(a) = 0 \).

**Proof.** We can assume that \( R = k \) is a field.

4.8 Discriminant of projective curves

Let \( C \subset \mathbb{P}^2 \) be a curve over the ring \( R \). We define its discriminant ideal to be the ideal generated by all discriminant ideals of \( C \) in some affine coordinates.

**Exercise 28** Let us take the curve \( y^2z - x^3 - 17z^3 = 0 \) over \( \mathbb{Z} \). Its discriminant in the affine coordinates \( z = 1 \), respectively \( y = 1 \), is \( 2 \cdot 3 \cdot 17^2 \), respectively \( 2^4 \). Its discriminant is \( 2^4 \cdot 3 \cdot 7^2 \) (see the tex file of this text for the corresponding Singular code).
4.9 Curves of genus zero

Let \( f \in k[x, y] \) and let \( C \) be the curve induced by \( f = 0 \) in \( \mathbb{P}^2 \). Let us assume that \( f \) is of degree 2 and it is irreducible over \( \bar{k} \). Further, assume that \( C(k) \) has at least one point \( P \). Note that if we look \( C \) in an affine chart then this point can be a point at infinity. The following procedure finds all the points of \( C(k) \). We fix a line \( L \) in \( \mathbb{P}^2 \), for instance take \( y = 0 \). For any point \( X \in L(k) \), we connect \( X \) to \( P \) by a line \( L' \) and find the second intersection \( f(X) \) of \( L' \) with \( L \). Since \( P \in C(k) \), we have \( f(X) \in C(k) \) and we get a bijection

\[
 f : L(k) \to C(k)
\]

Exercise 29 Use the above geometric argument and find all \( k \)-rational points of the Diophantine equation

\[
 tx^2 + sy^2 = t + s.
\]

for some \( s, t \in k \).

The argument discussed in the previous paragraph works if \( f \in k[x, y] \) is irreducible over \( \bar{k} \) and has degree 3 and the induced curve \( C \) in \( \mathbb{P}^2 \) is singular. In this case, we can prove that the singularity \( P \) of \( C \) is defined over \( k \), that is \( P \in C(k) \), and it is unique. This point serves us as the point with the same name in the previous paragraph.

Exercise 30 Find all the \( k \)-rational points of the Diophantine equation

\[
 y^2 - x^3 - t_4 x - t_6 = 0
\]

for some \( t_4, t_6 \in k \) with \( 4t_4^3 + 27t_6^2 = 0 \).

4.10 Curves of genus bigger than one

Let \( C/\mathbb{Q} \) be a smooth projective curve of degree \( d \) in \( \mathbb{P}^2 \), i.e. its defining polynomial is of degree \( d \). Its genus is by definition

\[
 g(C) := \frac{(d - 1)(d - 2)}{2}
\]

The main objective of the Diophantine theory is to describe the set \( C(\mathbb{Q}) \) for the curves defined over \( \mathbb{Q} \). The most famous example is the Fermat curve given by the polynomial \( f = x^n + y^n - 1 \). The machinery of algebraic geometry is very useful to distinguish between various types of Diophantine equations. For instance, one can describe the rational points of genus zero curves. Genus one curves are called elliptic curves and the study of their rational points is the objective of the present text. For higher genus we have a conjecture of Mordell around 1922 which is proved by Faltings in 1982:
4.12 Elliptic curves in Weierstrass form

A non-singular projective curve of genus $> 1$ and defined over $\mathbb{Q}$ has only finitely many $\mathbb{Q}$-rational points.

In fact, the above theorem is true even for number fields. For instance the above theorem says that the Fermat curve $F_n$ has a finite number of $\mathbb{Q}$-rational points. However, it does not say something about the nature of $F_n(\mathbb{Q})$. Mordell’s conjecture for function fields was proved by Y. Manin in 1963, see [Man63].

4.11 Elliptic curves in Weierstrass form

In this chapter, we define what is an elliptic curve over a field $k$, we describe the Weierstrass format of an elliptic curve and we define the group structure of an elliptic curve. If the reader is not familiar with the notion of an a curve over a field, he can use the curves in $\mathbb{P}^2$ which we worked out in the previous section.

We are ready to give the definition of an elliptic curve:

**Definition 4.11.1** An elliptic curve over $k$ is a pair $(E, O)$, where $E$ is a genus one complete smooth curve and $O$ is a $k$-rational point of $E$, that is, $O \in C(k)$.

Therefore, by definition an elliptic curve over $k$ has at least one $k$-rational point. A smooth projective curve of degree 3 is therefore an elliptic curve if it has a $k$-rational point. For instance, the Fermat curve $F_3 : x^3 + y^3 = z^3$ is an elliptic curve over $\mathbb{Q}$. It has $\mathbb{Q}$-rational points $[0, 1, 1]$ and $[1, 0, 1]$. However $E : 3x^3 + 4y^3 + 5z^3 = 0$ has not $\mathbb{Q}$-rational points and so it is not an elliptic curve defined over $\mathbb{Q}$. It is an interesting fact to mention that $E(\mathbb{Q}_p)$ for all prime $p$ and $E(\mathbb{R})$ are not empty. This example is due to Selmer (see [Cas66, Sel51]).

4.12 Elliptic curves in Weierstrass form

An elliptic curve in the Weierstrass form $E$ is the affine curve given by the polynomial

$$E_{t_2,t_3} : y^2 - x^3 - t_2 x - t_3, \quad t_2, t_3 \in k,$$

$$\Delta := 2(4t_2^3 + 27t_3^2) \neq 0,$$

and in particular $k$ is not of characterestic 2. In homogeneous coordinates it is written in the form

$$zy^2 - x^3 - t_2 x z^2 - t_3 z^3 = 0.$$
It has only one point at infinity, namely \([0; 1; 0]\), which is considered as the marked point in the definition of an elliptic curve. It is in fact a smooth point of \(\bar{E}\) which is tangent to the projective line at infinity of order 3 and \([0; 1; 0]\) is the only intersection point of the line at infinity with \(\bar{E}\). If \(\text{char}(k) = 2\) then the curve \(E_{t_2, t_3}\) is always singular. We have already seen in Proposition 4.7.1 that \(\Delta = 0\) if and only if the corresponding curve is singular.

### 4.13 Real geometry of elliptic curves

For a projective smooth curve \(C\) defined over \(\mathbb{R}\) the set \(C(\mathbb{R})\) has many connected components, all of them topologically isomorphic to a circle. We call each of them an oval.

For an elliptic curve \(E\) defined over \(\mathbb{R}\) we want to analyze the topology of \(E(\mathbb{R})\). For simplicity (in fact because of Proposition 4.18.1 which will be presented later) we assume that \(E = E_{t_2, t_3}\) is in the Weierstrass form. For \((t_2, t_3) \in \mathbb{R}^2\) let \(\Delta = 2(4t_2^3 + 27t_3^2)\) be the discriminant of the elliptic curve \(E\). We have:

1. If \(\Delta < 0\) then \(E(\mathbb{R})\) has two connected components, one is a closed path in \(\mathbb{R}^2\), which we call it an affine oval, and the other a closed path in \(\mathbb{P}^2(\mathbb{R})\). We call it a projective oval.
2. If \(\Delta > 0\) then \(E(\mathbb{R})\) has only one component which is a projective oval.
3. If \(\Delta = 0\) and \(t_3 < 0\) then \(E(\mathbb{R})\) is an \(\alpha\)-shaped path in \(\mathbb{R}^2\) (\(\infty\)-shaped path in \(\mathbb{P}^2(\mathbb{R})\)). In this case, we say that \(E\) has a real nodal singularity.
4. If \(\Delta = 0\) and \(t_3 > 0\) then \(E(\mathbb{R})\) is a union of a point and a projective oval. In this case, we say that \(E\) has a complex nodal singularity.
5. If \(t_2 = t_3 = 0\) then \(E(\mathbb{R})\) look likes a broken line in \(\mathbb{R}^2\). In this case, we say that \(E\) has a cuspidal singularity.

Note that \(E(\mathbb{R})\) intersects the line at infinity only at \([0; 1; 0]\). To see/prove all the topological statements above, it is enough to take an example in each class and draw the corresponding \(E(\mathbb{R})\). Note that in the \((t_2, t_3)\)-space each set defined by the above items is connected and the topology of \(E(\mathbb{R})\) does not change in each item (see Figures 4.1 and 4.2, the correspondence between the values of \(t_2, t_3\) and \(E_{t_2, t_3}(\mathbb{R})\) are done by colours).

### 4.14 Complex geometry of elliptic curves

Let \(C\) be a smooth projective curve of genus \(g\) over a subfield \(k\) of \(\mathbb{C}\). It can be shown that \(C(\mathbb{C})\) is a compact (Riemann) surface with \(g(C)\) wholes (a sphere with \(g\) handles).
4.15 The group law in elliptic curves

**Fig. 4.1** Elliptic curves: $y^2 - x^3 - tx^2 - t = 0$

**Fig. 4.2** The discriminant curve $4t^3 + t^2 = 0$

**Exercise 31** Give a proof of the above statement using the followings. 2. Any compact Riemann surface is diffeomorphic to a sphere with some handles. 2. Riemann-Hurwitz formula.

In genus one case, therefore, the set $C(\mathbb{C})$ is torus.

**Exercise 32** For a smooth elliptic curve $E$ over $\mathbb{R}$ and in the Weierstrass form describe the real curves $E(\mathbb{R})$ inside the torus (Hint: Use the Riemann-Hurwitz formula).

### 4.15 The group law in elliptic curves

Let $C$ be a smooth cubic curve in $\mathbb{P}^2$. Let also $P, Q \in C(k)$ and $L$ be the line in $\mathbb{P}^2$ connecting two points $P$ and $Q$. If $P = Q$ then $L$ is the tangent line to $C$ at $P$. The line $L$ is defined over $k$ and it is easy to verify that the third intersection $R := PQ$ of $C(\bar{k})$ with $L(\bar{k})$ is also in $C(k)$. Fix a point $O \in C(k)$ and call it the zero element of $C(k)$. Define

$$P + Q = O(PQ)$$
For instance, for an elliptic curve in the Weierstrass form take \( O = [0; 1; 0] \) the point at infinity. By definition \( O + O = O \).

**Theorem 4.15.1** The above construction turns \( C(k) \) into a commutative group.

**Proof.** The only non-trivial piece of the proof is the associativity property of +:

\[
(P + Q) + R = P + (Q + R)
\]

The proof constitute of three pieces:

1. Let \( P_i = [x_i; y_i; z_i] \) be 8 points in \( \mathbb{P}^2(\bar{k}) \) such that the vectors \( (x_i^3, \ldots, z_i^3) \in \bar{k}^{10} \) of monomials of degree 3 in \( x_i, y_i, z_i \) are linearly independent. A cubic polynomial \( F \) passing through all \( P_i \)'s corresponds to a vector \( a \in \bar{k}^{10} \) such that \( P_i \cdot a = 0 \) and so the space of such cubic polynomials is two dimensional. This means that there is two cubic polynomial \( F \) and \( G \) such that any other cubic polynomial passing through \( P_i \)'s is of the form \( \lambda F + \mu G \) and so it crosses a ninth point too.

2. We apply the first part to the eight points \( O, P_i, Q_i, R_i, PQ, QR, P + Q, Q + R \) and conclude that \( (P + Q)R = P(Q + R) \). Note that from these 8 points it crosses there cubic polynomials: \( C \), the product of lines through \( (0, PQ, P + Q), (R, Q, QR), (P(Q + R), P, Q + R) \) and the product of the lines \( (0, QR, Q + R), (PQ, Q, P), (P + Q, R, (P + Q)R) \):

\[
\begin{pmatrix}
P + Q & PQ & O \\
R & Q & QR \\
(P + Q)R, P(Q + R) & P + Q + R
\end{pmatrix}
\]

(each column or row corresponds to aline).

3. The morphisms \( C \times C \times C \rightarrow C, (P, Q, R) \mapsto (P + Q) + R, P + (Q + R) \) coincides in a Zariski open subset and so they are equal.

**Exercise 33** [Si92] p. 60) On the elliptic curve

\[
E : y^2 = x^3 + 17
\]

over \( \mathbb{Q} \). We have points

\[
P_1 = (-2, 3), \ P_2 = (-1, 4), \ P_3 = (2, 5), \ P_4 = (4, 9), \ P_5 = (8, 23)P_6 = (43, 282)
\]

\[
P_7 = (52, 375), \ P_8 = (5234, 378661)
\]

verify:

\[
P_8 = 2P_1, \ P_4 = P_1 - P_3, \ 3P_1 - P_3 = P_7,
\]

Prove that \( E(\mathbb{Q}) \) is freely generated by \( P_1 \) and \( P_3 \) and there are only 16 integral points \( \pm P_i, i = 1, 2, \ldots, 8 \) (see [Nag35]).

**Exercise 34** [Kob93], p. 35, Problem 4b: For the elliptic curve \( E_n : y^2 = x^3 - n^2x \) find an explicit formula for the \( x \) coordinates of inflection points.

**Exercise 35** [Kob93], p. 36, Problem 7: How many elements of \( E_n(\mathbb{R}) \) or of order 2, 3 and 4? Describe geometrically where these points are located.
**Exercise 36** [Kob93], p. 36, Problem 9: For an elliptic curve over \( \mathbb{R} \) prove that \( E(\mathbb{R}) \) (as a group) is isomorphic to \( \mathbb{R}/\mathbb{Z} \) or \( \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

**Exercise 37** [Kob93], p. 36, Problem 11:

### 4.16 Divisors

Let \( E/k \) be an elliptic curve over a field \( k \). A divisor in \( E \) and defined over \( k \) is a formal finite sum \( D := \sum n_i p_i \), with \( n_i \in \mathbb{Z} \) such that it is invariant under the Galois group \( \text{Gal}(\bar{k}/k) \, that is, \)

\[
\sigma(D) = D, \quad \forall \sigma \in \text{Gal}(\bar{k}/k)
\]

where

\[
\sigma(\sum n_i p_i) := \sum n_i \sigma(p_i)
\]

The set of divisors over \( k \), let us denote it by \( \text{Div}(E/k) \) form an abelian group in a natural way. For any rational function \( f \in k(E) \) we define

\[
\text{div}(f) := \sum n_i p_i
\]

where \( f \) is of order \( n_i \) at \( p_i \). It is a divisor defined over \( k \). The set of such divisors form an abelian group which we denote it by \( \text{Div}(k(E)) \). The Picard-Group of \( E \) is defined to be

\[
\text{Pic}(E) := \text{Div}(E)/\text{Div}(k(E)).
\]

The Chern class map is defined in the following way

\[
c : \text{Pic}(E) \to \mathbb{Z}, \quad c(\sum n_i p_i) := \sum n_i
\]

we define

\[
\text{Pic}_0(E) := \ker(\text{Pic}(E) \to \mathbb{Z})
\]

We have a canonical map

\[
E(k) \to \text{Pic}_0(E), \quad P \mapsto P - O
\] (4.7)

**Proposition 4.16.1** The map (4.7) is an isomorphism of groups.

**Proof.** First of all we notice that it is a group morphism. Just for this proof we denote by \( \oplus \) the addition structure in \( E(k) \). Let \( L_1 \), respectively \( L_2 \), be the equation of the line in \( \mathbb{P}^2 \) passing through \( P, Q, PQ \), respectively \( O, PQ, P \oplus Q \). We have \( \frac{L_1}{L_2} \in k(E) \) with the divisor
\[ P + Q + PQ - O - PQ - P \oplus Q \]
and so in \( \text{Pic}_0(E) \) we have \( P - O + Q - O = P \oplus Q - O \).

### 4.17 Riemann-Roch theorem

**Definition 4.17.1** We say that a divisor \( D = \sum n_i p_i \) is positive and write \( D \geq 0 \) if all coefficients \( n_i \) are non negative integers. In a similar way we define \( D \leq 0 \).

For a divisor \( D \) on a curve \( C/k \) define the linear system
\[
\mathcal{P}(D) = \{ f \in k(C), f \neq 0 \mid \text{div}(f) + D \geq 0 \} \cup \{0\}
\]
and
\[
l(D) = \dim_k(\mathcal{P}(D)).
\]

**Theorem 4.17.1** (Riemann-Roch theorem) Let \( C \) be a smooth curve over \( k \).

\[
l(D) - l(K - D) = \deg(D) - g + 1,
\]
where \( K \) is the canonical divisor and \( g \) is the genus of \( C \).

We only need to know that the canonical divisor satisfies:

\[
\deg(K) = 2g - 2
\]
and so for \( \deg(D) > 2g - 2 \), equivalently \( \deg(K - D) < 0 \), we have

\[
l(D) = \deg(D) - g + 1. \tag{4.8}
\]

### 4.18 Weierstrass form revised

In this section we prove that any elliptic curve can be realized as a certain curve in \( \mathbb{P}^2 \). The following proposition is proved in [Sil92], III, Proposition 3.1.

**Proposition 4.18.1** Let \( E \) be an elliptic curve over a field \( k \). There exist functions \( x, y \in k(E) \) such that the map

\[
E \rightarrow \mathbb{P}^2, \ a \mapsto [x(a); y(a); 1]
\]
give an isomorphism of \( E/k \) onto a curve given by

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \ a_1, \ldots, a_6 \in k
\]
sending $O$ to $[0; 1; 0]$. If further $\text{char}(k) \neq 2, 3$ we can assume that the image curve is given by

$$y^2 = 4x^3 - t_2x - t_3, \quad t_2, t_3 \in k, t_2^3 - 27t_3^2 \neq 0.$$ 

We call $x$ and $y$ the Weierstrass coordinates of of $E$.

**Proof.** Using Riemann-Roch theorem and in particular (4.8) with $g = 1$ and $D = nO$ we get $l(D) = n$. For $n = 2$ we can choose $x, y \in k(E)$ such that $1, x$ form a basis of $\mathcal{P}(2O)$ and $1, x, y$ form a basis of $\mathcal{P}(3O)$. The function $x$ (resp. $y$) has a pole of order 2 (resp. 3) at $O$. Now $\mathcal{P}(6O)$ has dimension 6 and $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{P}(6O)$. It follows that there is a relation

$$a_1y^2 + a_1xy + a_2y = bx^3 + a_2x^2 + a_4x + a_6, \quad a_1, \cdots, a_6, a, b \in k.$$ 

Note that $ab \neq 0$, otherwise every term would have a different pole order at $O$ and so all the coefficients would vanish. Multiplying $x, y$ with some constants and dividing the whole equation with another constant, we get the desired equation. The map induced by $x$ and $y$ is the desired map (check the details).

If $\text{char}(k) \neq 2, 3$ we make the change of variables $x' = x, y' = y - \frac{a_1x}{2}$ and we eliminate $xy$ term. A change of variables $x' = x - \frac{a_2}{3}, \quad y' = y - \frac{a_4x}{2}$ will eliminate $x^2$ and $y$ terms.

**Exercise 38** Write the following elliptic curves in the Weierstrass form:

$$y^2 = x^4 - 1, \quad O = [0; 1; 0]$$

$$x^3 + y^3 = 1, \quad O = [0; 1; 1]$$

### 4.19 Moduli of elliptic curves

Now we can state what is the moduli of elliptic curves.

**Proposition 4.19.1** Assume that $\text{char}(k) \neq 2, 3$. Two elliptic curves $E_{t_2,t_3}$ and $E_{t_2',t_3'}$ are isomorphic if and only if there exists $\lambda \in k$, $\lambda \neq 0$ such that

$$t_2' = \lambda^4t_2, \quad t_3' = \lambda^6t_3$$

The isomorphism is given by

$$(x,y) \mapsto (\lambda^2x, \lambda^3y).$$

**Proof.** Let $(x, y)$ and $(x', y')$ be two sets of Weierstrass coordinate functions on an elliptic curve $E_{t_2,t_3}$. It follows that $\{1, x\}$ and $\{1, x'\}$ are both bases of $\mathcal{P}(2O)$, and similarly $\{1, x, y\}$ and $\{1, x', y'\}$ are both bases for $\mathcal{P}(3O)$. Writing $x', y'$ in terms of $x, y$ and substituting in the equation of $E_{t_2',t_3'}$ we get the first affirmation of the proposition. The second affirmation is easy to check.
Combining Proposition 4.18.1 and Proposition 4.19.1 we conclude that the moduli space of elliptic curves over a field of characteristic \( \neq 2, 3 \) is

\[
\mathcal{M}_1(k) := (\mathbb{A}^2(k) - \{(t_2, t_3) \mid 4t_2^3 + 27t_3^2 = 0\}) / \sim
\]

where

\[(t_2, t_3) \sim (t'_2, t'_3) \text{ if and only if } \exists \lambda \in k, \lambda \neq 0, (t'_2, t'_3) = (\lambda^4 t_2, \lambda^6 t_3).\]

If \( k \) is algebraically closed then this is the set of \( k \)-rational points of the weighted projective space \( \mathbb{P}^{2,3}(k) \) minus a point induced in \( \mathbb{P}^{2,3} \) by \( \Delta = 0 \). In this case the \( j \)-invariant of elliptic curves

\[
j : \mathcal{M}_1(k) \to \mathbb{A}(k), \quad j[t_2; t_3] = \frac{1728 \cdot 4t_3^2}{4t_2^3 + 27t_3^2}
\]

is an isomorphism and so the moduli of elliptic curves over \( k \) is \( \mathbb{A}^1(k) \). However, note that if \( k \) is not algebraically closed then \( j \) has non-trivial fibers. For instance, all the elliptic curves

\[y^2 = x^3 - t_3, \quad t_3 \in \mathbb{Q}\]

are isomorphic over \( \overline{\mathbb{Q}} \) but not over \( \mathbb{Q} \).

If \( j_0 \neq 0, 1728 \) consider the elliptic curve:

\[E_{j_0} : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.
\]

It satisfies \( j(E) = j_0 \).

### 4.20 The addition formula for \( \wp \)

For a fixed \( z' \in \mathbb{C}, \ z' \neq 0 \), let us consider \( \wp(z + z') \) which is double periodic in \( z \), and hence, it is a rational function in \( \wp \) and \( \wp' \)

**Proposition 4.20.1** We have

\[
\wp(z + y) = \frac{1}{4} \left( \frac{\wp(z) - \wp'(y)}{\wp(z) - \wp(y)} \right)^2 - \wp(z) - \wp(y) \tag{4.9}
\]

**Proof.** Let \( f(z) \) be the difference between the left and the right hand sides of 4.9. Its only possible poles are in

\[z = 0, \pm y\]

We examine the Laurent expansion of \( f(z) \) at the point \( z = 0 \) and see that it is holomorphic at \( z = 0 \) and there it vanishes. In a similar way, it has no poles at \( z = y \).
4.20 The addition formula for \( \wp \)

and so, at worst it has a simple pole at \( z = -y \). Since \( f \) is double periodic we get the result.

We let \( y \) goes to \( z \) and we get

\[
\wp(2z) = \frac{1}{4} \left( \frac{\wp'(z)}{\wp(z)} \right)^2 - 2\wp(z).
\]

If we make derivation of 4.9 with respect to \( z \) we get a similar formula for \( \wp(x+y) \).

A better organization of this formula is

\[
\begin{vmatrix}
\wp(z), & \wp'(z) \\
\wp(y), & \wp'(y) \\
-\wp(x+y), & \wp'(z+y)
\end{vmatrix} = 0
\]

Note that we can state the same formulas in the algebraic context, that is, for an elliptic curve \( E \) over the field \( k \) with the Weierstrass coordinates \( x \) and \( y \) we have

\[
x(P + Q) = \frac{1}{4} \left( \frac{y(P) - y(Q)}{x(P) - x(Q)} \right)^2 - x(P) - y(Q) \tag{4.10}
\]

\[
\begin{vmatrix}
x(P), & y(P) \\
x(Q), & y(Q) \\
-x(P + Q), & y(P + Q)
\end{vmatrix} = 0 \tag{4.11}
\]

\[
x(2P) = \frac{1}{4} \left( \frac{6x(P) - 1}{y(P)} \right)^2 - 2x(P) \tag{4.12}
\]

Even though, we have proved 4.10, 4.11, 4.12 in the complex context, they are valid for an elliptic curve over an arbitrary field. The argument for instance for 4.11 is as follows: We consider \( g_2, g_3, x(P), y(P), x(Q), y(Q), x(P + Q), y(P + Q) \) as variables. The equation 4.11 is in fact a collection of equations:

\[
\begin{align*}
y(P)^2 &= 4x(P)^2 - g_2x(P) - g_3 \\
y(Q)^2 &= 4x(Q)^2 - g_2 \cdot x(Q) - g_3
\end{align*}
\]

The equation of line \( \ell \) passing through \( P, Q \)

\[
\begin{align*}
y(P + Q)^2 &= 4x(P + Q)^3 - g_2 \cdot x(P + Q) - g_3
\end{align*}
\]

This is a variety defined over \( \mathbb{Z} \left[ \frac{1}{6} \right] \)
4.21 Why Schemes?

One of the fundamental observations in Grothendieck’s revolution of Algebraic Geometry, replacing varieties with schemes, is that

\[ \text{Spec}(\mathbb{Z}) := \{ \text{prime ideals of } \mathbb{Z} \} \simeq \{2, 3, 5, \ldots, p, \ldots\} \]

is like a parameter, for instance, the parameter \( \lambda \) in the legendary family of elliptic curves:

\[ E_\lambda : y^2 = 4\chi(2-1)(\chi - \lambda), \lambda \in \mathbb{C} \]

We consider \( E_\lambda \) as a curve over the ring \( \mathbb{C}[\lambda] := \text{polynomials in } \lambda \text{ with } \mathbb{C} -\text{coefficients} \).

The prime ideals of \( \mathbb{C}[\lambda] \) are

\[ \text{Spec}(\mathbb{C}[\lambda]) := \{ (\lambda - \lambda_0)\mathbb{C}[\lambda] \mid \lambda_0 \in \mathbb{C} \} \simeq \mathbb{C} \]

For a prime ideal \( P \subseteq \mathbb{C}[\lambda] \), the residue field is naturally isomorphic to \( \mathbb{C} \)

\[ \mathbb{C}[\lambda]/(\lambda - \lambda_0)\mathbb{C}[\lambda] \overset{\sim}{\longrightarrow} \mathbb{C} \]

\[ p(\lambda) \longmapsto P(\lambda_0) \]

The process of substituting \( \lambda \) with \( \lambda_0 \), can be interpreted as considering \( E_\lambda \) over the residue field. In a similar way for an elliptic curve over \( \mathbb{Z} \), for instance

\[ E : y^2 = x^3 + 1 \]

The process of working modulo a prime number \( p \) is the same as considering \( E \) over the residue field

\[ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \]

Another reason for using schemes is that defining ideal of affine varieties have more data than the underlying variety. For instance, the underlying variety of the ideal \( I = \langle x, xy \rangle \subset k[x, y] \) is just \( \{x = 0\} \), however, we have \( I = \langle x \rangle \cap \langle x, y \rangle \) which means that we must look at the underlying variety as a union of \( \{x = y = 0\} \) and \( \{x = 0\} \).
Chapter 5
Mordell-Weil Theorem

We have seen that for an elliptic curve over $\mathbb{Q}$ the set $E(\mathbb{Q})$ is an abelian group and so

$$E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$$

where

$$E(\mathbb{Q})_{\text{tors}} := \{ x \in E(\mathbb{Q}) \mid nx = 0, \text{ for some } n \in \mathbb{N} \},$$

is a freely generated $\mathbb{Z}$-module.

**Theorem 5.0.1** For an elliptic curve $E$ over a number field $k$ the group $E(k)$ of $k$-rational points is finitely generated abelian group.

The above theorem for $k = \mathbb{Q}$ was proved by Mordell. Its generalization for an arbitrary number field was proved by André Weil and it is known as the Mordell-Weil theorem. For the proof see [Lan78a, Hus04].

Let us take $k = \mathbb{Q}$. The above theorem implies that the set of torsion points $E(\mathbb{Q})_{\text{tors}}$ of $E(\mathbb{Q})$ is finite and there is a number $r \in \mathbb{N}$ such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}.$$

The non-negative integer $r$ is called the rank of $E(\mathbb{Q})$.

**5.1 Mordell-Weil theorem**

The free part of $E(k)$, even for $k = \mathbb{Q}$, is mysterious. We do not know whether there exist an elliptic curve of arbitrary rank or not. Until 1977, only, elliptic curves of rank $\leq 9$ was known. This is somehow trivial. Then, Mestre rank $\leq 15$, Nago 1992-1994, rank=17, 20, 21, Fermigier, 1992-1997 rank 19, 20, Martin-McMiller, 1998-2000, rank=23, 24, and finally in 2006, N. Elkies found an elliptic curve of rank 28. This is the largest rank known until now. There are results saying that with probability 1, an elliptic curve $E/\mathbb{Q}$ has rank 0 or 1.
Proof of Mordell’s theorem consists of two steps

\[
\begin{cases}
E(Q)/2E(Q) & \text{is finite (Weak Mordell)} \\
\text{Existence of a height function}
\end{cases}
\]

**Theorem 5.1.1** (descent theorem). Let \( \Gamma \) be a commutative group. Suppose that there is a function

\[ h : \Gamma \to [0, \infty) \]

such that

1. For any real number \( M \), the set \( P \in \Gamma | h(P) \leq M \) is finite.
2. For every \( P_0 \in \Gamma \), there is a constant \( k_0 \) such that

\[ h(P + P_0) \leq 2h(P) + k_0 \quad \forall P \in \Gamma \]

3. There is a constant \( k \) such that

\[ h(2P) \leq 4h(P) - k \quad \forall P \in \Gamma \]

Then \( \Gamma \) is finitely generated.

**Proof.** Let \( \Gamma/2\Gamma = Q_1, Q_2, \ldots, Q_n \). It means that for every \( P \in \Gamma \exists Q_{i_1}, \) depending on \( P \) such that

\[ P - Q_{i_1} = 2P_2 \in 2\Gamma \]

We repeat this for \( P_2 \).

\[
\begin{align*}
P - Q_{i_1} &= 2P_1 \\
P_1 - Q_{i_2} &= 2P_2 \\
&\vdots \\
P_{m-1} - Q_{i_m} &= 2P_m
\end{align*}
\]

This implies that

\[ P = Q_{i_1} + 2Q_{i_2} + 2^2Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^mP_m \]

Now we use the height function. We have

\[ h(P - Q_i) \leq 2h(P) + k' \quad \forall P \in \Gamma \quad i = 1, \ldots, n \]

Where \( k' \) is the maximum of \( k_i \)'s attached to each \( Q_i \) in property 2 of \( h \). We use property 3 of \( h \) and we have
5.1 Mordell-Weil theorem

\[ 4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{j-1}) + k \]
\[ \leq 2h(P_{j-1}) + k' + k \implies \]
\[ h(P_j) \leq \frac{1}{2} h(P_{j-1}) + \frac{k + k'}{4} \]
\[ = \frac{3}{4} h(P_{j-1}) - \frac{1}{4} \left( h(P_{j-1}) - (k + k') \right) \]

Therefore, if \( h(P_{j-1}) \geq k' + k \) then
\[ h(P_j) \leq \frac{3}{4} h(P_{j-1}) \]

We do this process until for some \( m \) \( h(P_m) \leq k' + k \) and so by property 1 of \( h \) the set of such \( P_m \) is finite. We conclude that \( \Gamma \) is generated by \( Q_1, Q_2, \ldots, Q_n \), \( \{ P \in \Gamma \mid h(P) \leq k' \} \)

Now, let us construct the height function for \( E(Q) \). Let \( P = (x, y) \in E(Q) \). Write
\[ x := \frac{m}{n}, \ (m,n) = 1 \]
\[ H(P) := H(x) = \max\{|m|, |n|\} \]
\[ h(P) := \log H(P) \]

Let \( P = (x, y) = \left( \frac{m}{e^2}, \frac{n}{e^3} \right) \), \( m, n, e \in \mathbb{Z} \). We have
\[ |n|^2 \leq |m|^3 + \left| t_2 \right| e^4 |m| + \left| t_3 \right| e^6 \]
\[ \leq k^2 H(P)^3 \implies |n| \leq kH(P)^{\frac{1}{2}} \]

Where \( k \) is a constant number which only depends on \( E \). Let \( P = (x, y), P_0 = (x_0, y_0) \). We would like to estimate \( h(P + P_0) \).

\[ h(P + P_0) = \left( \frac{y - y_0}{x - x_0} \right)^2 - x - x_0 \]
\[ = \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0)}{(x - x_0)^2} \]
\[ = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \]

Here, we have used \( y^2 = x^3 - t_2x - t_3 \) and \( A, B, \ldots, G \) are constants depending only on \( E \) and \( P_0 \). Now set \( P = \left( \frac{m}{e^2}, \frac{n}{e^3} \right) \), \( (m, e^2) = 1 \) and \( (n, e^3) = 1 \)
\[ H(P + P_0) \leq \max \{|A P_n + B m^2 + C m e^2 + D e^4|, |E m^2 + F m e^2 + G e^4|\} \]

But, we know that

\[ |e| \leq H(P)^{1/2}, |n| \leq k \cdot H(P)^{1/2}, |m| \leq H(P) \]

Which implies that

\[ H(P + P_0) \leq \text{constant}. H(P)^2 \]

Where the constant term depends only on \( E \) and \( P_0 \). Taking the logarithm of this, we have the property 2 of \( h \).

Let us prove property 3 of \( h \). We have

\[ x(2P) = \frac{f'(x)}{4f(x)} - 2x \]

Where \( y^2 = x^3 - t_2 x - t_3 = f(x) \) is the elliptic curve \( E \) We assume that \( 2P \neq 0 \)

\[ x(2P) = \frac{P(x)}{Q(x)}, \text{deg } P(x) = 4, \text{deg } Q(x) = 3 \]

Where the coefficients of \( P, Q \) only depends on the elliptic curve.

Let \( 4(4t_2^3 + 27t_2^2) \) This is the resultant of \( P(x) \) and \( Q(x) \). This means that

\[ f_1(x) P(x) + f_2(x) Q(x) = \Delta \]

\[ f_1, f_2 \in \mathbb{Z}[x], \text{deg } f_1, \text{deg } f_2 \leq 3 \]

We need also

\[ g_1(x) P(x) + g_2(x) Q(x) = \Delta \cdot x^7 \]

\[ g_1, g_2 \in \mathbb{Z}[x], \text{deg } g_1, \text{deg } g_2 \leq 3 \]

This can be considered as the resultant of \( x^4 P \left( \frac{1}{x} \right), x^4 Q \left( \frac{1}{x} \right) \)

Let \( x = \frac{a}{b}, (a, b) = 1 \) and

\[ x(2P) = \frac{F(a, b)}{G(a, b)}, \quad \delta := \left( F(a, b), G(a, b) \right) \]

Therefore,

\[ f_1(a, b) F(a, b) + f_2(a, b) G(a, b) = 4\Delta b^7 \]

\[ g_1(a, b) F(a, b) + g_2(a, b) G(a, b) = 4\Delta a^7 \quad (5.1) \]

This gives

\[ \delta |4\Delta \quad \text{and} \quad |\delta| \leq |4\Delta| \]

and so
5.1 Mordell-Weil theorem

\[ H(2P) \geq \max \{ |F(a,b)|, |G(a,b)| \} / |4\Delta| \]

On the other hands

\[ |4\Delta b^7| \leq 2 \max \{ |f_1|, |f_2| \} \max \{ |F|, |G| \} \] \hspace{1cm} (5.2)

\[ |4\Delta a^7| \leq 2 \max \{ |g_1|, |g_2| \} \max \{ |f|, |G| \} \]

Where \( f_1, f_2 \ldots \) are evaluated at \((a,b)\).

Now \( f_1, f_2, g_1, g_2 \) are polynomials of degree \( \leq 3 \).

\[ \max \{ |f_1|, |f_2|, |g_1|, |g_2| \} \leq C \max \{ |a|^3, |b|^3 \} \] \hspace{1cm} (5.3)

Where \( C \) is a constant which only depends on \( E \). Combining (5.2) and (5.3) we get

\[ |4\Delta| \max \{ |a^7|, |b^7| \} \leq 2C \cdot \max \{ |a|^3, |b|^3 \} \max \{ |F(a,b)|, |G(a,b)| \} \]

and so

\[ H(2P) = \frac{\max(|F(a,b)|,|G(a,b)|)}{4\Delta} \geq \frac{\max(|F(a,b)|,|G(a,b)|)}{4\Delta} \]

\[ \geq (2C)^{-1}\max \{ |a|, |b| \} = (2C)^{-1}H(P) \]

For more on descent procedure see [Silvermann I] page 199 chapter VIII.

**Proposition 5.1.1** Let \( E \) be an elliptic curve over \( \mathbb{Q} \). We have

\[ h(P_1 + P_2) + h(P_1 - P_2) \leq 2h(P_1) + 2h(P_2) + k \] \hspace{1cm} (5.4)

Where \( k \) only depends on \( E \).

For a proof see [Silvermann I] page 216.

**Proposition 5.1.2** (Tate). Let \( E/\mathbb{Q} \) be an elliptic curve

\[ \hat{h}(P) := \frac{1}{2} \lim_{N \to \infty} 4^{-N}h(2^NP) \]

exists.

**Proof.** Taken from [Silvermann I] page 288. We show that the sequence in \( \lim \) is Cauchy. In \([5.4]\) we pu \( P = P_1 = P_2 \)

\[ |h(2P) - 4h(P)| \leq k \]

Where \( k \) is a constant depending only on \( k \). For \( N \geq M \geq 0 \) integers, we have

\[ \left| 4^{-N}h(2^NP) - 4^{-M}h(2^MP) \right| = \left| \sum_{n=M}^{N-1} 4^{-n-1} h(2^{n+1}P) - 4^{-n} h(2^nP) \right| \]

\[ \leq \sum_{n=M}^{N-1} 4^{-n-1} \left| h(2^{n+1}P) - 4h(2^nP) \right| \leq \sum_{n=M}^{N-1} 4^{-n-1} C \]

\[ \leq \frac{C}{4^{N-M}} \]
Definition 5.1.1 \( \hat{h} \) is called the canonical or Neron-Tate height of \( E \).

Theorem 5.1.2 (Neron-Tate) The canonical height \( \hat{h} \) satisfies

1. For all \( P, Q \in E(\mathbb{Q}) \)
   \[ \hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q) \]

2. For all \( P \in E(\mathbb{Q}) \) and \( m \in \mathbb{Z} \)
   \[ \hat{h}(M, P) = m^2 \hat{h}(P) \]

3. \( \hat{h} \) is a quadratic form in \( E(\mathbb{Q}) \), that is, \( \hat{h} \) is even and the paring
   \[ \langle \cdot , \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R} \]
   \[ \langle P, Q \rangle = \hat{h}(P, Q) - \hat{h}(P) - \hat{h}(Q) \]
   is bilinear.

4. For \( P \in E(\mathbb{Q}) \) we have \( \hat{h}(P) \geq 0 \) and
   \[ \hat{h}(P) = 0 \iff P \text{ is a torsion point.} \]

5. \( 2\hat{h} - h \) is bounded on \( E(\mathbb{Q}) \).

Proof. Taken from [Silvermann I] page 229

5. We have
   \[ \left| 4^{-N} h(2^N P) - 4^{-M} h(2^M P) \right| \leq \frac{C}{4^{M+1}} \]
   Take \( M = 0 \) and let \( N \to \infty \). We get
   \[ |2\hat{h}(P) - h(P)| \leq \frac{C}{4} \]

1. We have
   \[ h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1) \]
   replace \( P, Q \) by \( 2^N P, 2^N Q \) and multiply it with \( \frac{1}{2} \) \( 4^{-N} \) and then \( N \to \infty \).

2. We know that \( h(mP) - m^2 h(P) \) is bounded. Again replace \( P \) by \( 2^{-N} P \), multiply with \( 4^{-N} \) and \( N \to \infty \)

The rest is left to the reader.

Let \( P_1, P_2, \ldots P_\gamma \) be a basis of the free part of \( E(\mathbb{Q}) \) The regulator of \( E/\mathbb{Q} \) is defined

\[ R_{E/\mathbb{Q}} := \det |\langle P_i, P_j \rangle| \]
5.2 Weak Mordell-Weil theorem

**Theorem 5.2.1** Let $E$ be an elliptic curve over a number field $k$. Then $E(k)/mE(k)$ is finite for all $m \in \mathbb{N}$.

We give a proof of weak Mordell-Weil theorem for $k = \mathbb{Q}$, the family

$E_{a,b}: y^2 = x^3 + ax^2 + bx$

and for $E(\mathbb{Q})/2E(\mathbb{Q})$. We follow Husemiller, chapter 6 3, in which he use an explicit 2-isogeny in chapter 4 5.
Chapter 6
Torsions and isogeny

6.1 Torsion points

Using Weierstrass theorem we have seen a correspondence

$$\text{The space of lattices } \rightarrow \text{ the space of pairs } (E, \omega)$$

(6.1)

Where $E$ is an elliptic curve over $\mathbb{C}$ and $\omega$ is a regular differential 1-form. Since we have not defined these objects intrinsically, then $E$ must be taken in the Weierstrass format an $\omega = \frac{dx}{y}$. In the right hand side of (6.1) we can talk about pairs defined over an arbitrary field.

**Definition 6.1.1** A pair $E, \omega$ is called an enhanced elliptic curve. There will be other enhancements, and in order to reduce confusion, we say that $E$ is enhanced with a regular differential 1-form.

**Definition 6.1.2** For an elliptic curve $E'$ over a field of characteristic zero $k$, the set of $m$-torsion in

$$E[m] = \{ P \in E(k) \mid mP = O \}$$

This is a subgroup of $E(k)$.

**Proposition 6.1.1** We have an embedding of groups

$$E[m] \hookrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

and for $k$ an algebraically closed field, this is an isomorphism.

**Proof.** We first prove the second part for $k = \mathbb{C}$. We can assume that $E = \mathbb{C}/\Lambda$ in this case

$$E[m] \simeq \frac{1}{m}\Lambda/\Lambda \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Now, we prove the second part. Since $k$ is a field of characteristic zero and $E$ uses a finite numbers of elements of $E$ we can assume that there is an embedding of fields
\[ \sigma : k \hookrightarrow \mathbb{C} \]

Let \( E_{\sigma} \) be the elliptic curve over \( \mathbb{C} \) obtained from \( E \) and regarding its coefficients as complex numbers. We have an embedding of groups

\[ E[m] \hookrightarrow E_{\sigma}[m] \cong \mathbb{Z}/m_\mathbb{Z} \times \mathbb{Z}/m_\mathbb{Z} \]

For \( k \) an algebraically closed field, the algebraic equation \( mP = O \) has \( m^2 \) distinct solution over \( \mathbb{C} \), and it is defined over \( k \). This means that all these solutions are defined over \( k \) and the result follows.

\[ \square \]

In particular, for an elliptic curve \( E \) over \( \mathbb{Q} \) we have

\[ E[m] \cong \mathbb{Z}/m_\mathbb{Z} \times \mathbb{Z}/m_\mathbb{Z} \]

Let

\[ E[2] = \{ (t_1, 0), (t_2, 0), (t_3, 0), O \} \]

For families of elliptic curves with a 3-torsion point see [Husemiller] Chapter 4, 2.

### 6.2 Isogeny

Let \( \Lambda \subseteq A \subseteq \mathbb{C} \) be two lattices and let

\[ N := \#A/\Lambda \]

This gives a map of tori

\[ f : \hat{E} \rightarrow E \quad (6.2) \]

Which is induced by the identity map \( \mathbb{C} \rightarrow \mathbb{C} \). Here, \( E = \mathbb{C}/\Lambda \) and \( \hat{E} = \mathbb{C}/\hat{\Lambda} \). This is actually a holomorphic map between two Riemann surfaces. It is as a morphism of groups. We have

\[ f^* \omega = \hat{\omega}, \]

where \( \omega \) and \( \hat{\omega} \) are the differential form \( dz \) induced in \( \hat{E} \), respectively. Furthermore

\[ f^{-1}([z]) = [z] + \frac{\Lambda}{A} \]

which means that \( f \) is a \( N \) to 1 map with no ramification points.

**Definition 6.2.1** \( f \) as in (6.2) is called an isogeny of degree \( N \).

**Definition 6.2.2** Let \( N := \#A/\Lambda \). we have

\[ NA \subseteq \hat{A} \subseteq A \]
and this gives us the maps

\[
E \xrightarrow{\bar{s}} \tilde{E} \xrightarrow{f} E
\]

\[
[z] \mapsto [Nz] \quad [z] \rightarrow [z]
\]

In the level of differential forms

\[
N\omega \leftarrow \tilde{\omega} \leftarrow \omega
\]

g is called the dual isogeny of f. Note that both \( F_{0g}, g_0f \) are multiplication by N map.

**Exercise 39** Let \( G \) be a finite abelian group generated by at most two elements. There are unique \( d_1, d_2 \in \mathbb{N} \) such that

\[
G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_1d_2\mathbb{Z}
\]

Conclude that any isogeny \( E_1 \mapsto E_2 \) can be uniquely written as

\[
E_1 \xrightarrow{\alpha} E_1 \xrightarrow{\beta} E_2
\]

\[
[z_1] \rightarrow [d_1z_1]
\]

Where \( \alpha \) is a multiplication by \( d_1 \) and \( \ker(\beta) \) is cyclic of order \( d_2 \).

Let \( a \in \mathbb{C}^* \) and \( \Lambda \subseteq \mathbb{C} \) be a lattice. Let also

\[
\tilde{E} = \mathbb{C}/a\Lambda, E = \mathbb{C}/\Lambda
\]

We have the map

\[
f_a : E \rightarrow \tilde{E} \quad [z] \mapsto [az]
\]

which is a bijection and its inverse is given by \( f_{a^{-1}} \). Moreover

\[
f_a^* \omega = a\tilde{\omega}
\]

Under the mentioned isomorphism, the lattices \( a\Lambda \) and \( \Lambda \) corresponds to \( (E, a\omega), (E, \omega) \).

**Exercise 40** Show that the number of sublattices \( \tilde{\Lambda} \subseteq \Lambda \) of a fixed lattice \( \Lambda \) with \( \#\Lambda/\tilde{\Lambda} = n \) is

\[
\sigma(n) = \sum_{d|n} d
\]

Hinit: Take a basis of \( \Lambda' \) and \( \Lambda \) and show that

\[
\tilde{\Lambda} \subseteq \Lambda, \quad \#\Lambda/\tilde{\Lambda} = n \longrightarrow SL(2, \mathbb{Z}) \backslash \text{Mat}_n(2, \mathbb{Z})
\]

\( \Lambda' \) generated by

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]

This quotient has representatives
\[
\begin{pmatrix}
a & b \\
c & d \\
\end{pmatrix}
0 \leq b \leq d - 1, \ a \cdot d = n
\]

Note that for \( n = P \) prime the set of such lattices is

\[
\hat{\Lambda} = \mathbb{Z}P\omega_1 + \mathbb{Z}\omega_2, \ \mathbb{Z}(\omega_1 + \omega_2) + \mathbb{Z}P\omega_2
0 \leq b \leq P - 1
\]

6.3 Isogeny II

Let \( E \) be an elliptic curve in the Weierstrass format and defined over \( \mathbb{Q} \), that is, \( t_2, t_3 \in \mathbb{Q} \). We have

\[
G := \Lambda/\hat{\Lambda} \subseteq E[n]
G \subseteq E(\mathbb{Q})
\]

We may think of \( E \) as the quotient \( E/G \). The elliptic curve \( \tilde{E} \) is also defined over \( \mathbb{Q} \) and the reason is as follows.

The pull-back of \( \varphi(z, \Lambda) \), \( \varphi(z, \hat{\Lambda}) \) by the map of isogeny is an elliptic function with respect to the lattice \( \hat{\Lambda} \). Therefore, we have

\[
\varphi(z, \Lambda) = P\left( \varphi(z, \hat{\Lambda}), \varphi'(z, \hat{\Lambda}) \right)
\varphi'(z, \Lambda) = Q\left( \varphi(z, \hat{\Lambda}), \varphi'(z, \hat{\Lambda}) \right)
\]

where \( P \) and \( Q \) are rational functions in two variables and with coefficients in \( \mathbb{C} \)

**Theorem 6.3.1** If \( E \) is defined over \( \mathbb{Q} \) then the isogeny

\[
\tilde{E} \to E \ \ (x, y) \to \left( P(x, y), Q(x, y) \right)
\]

is defined over \( \mathbb{Q} \), that is \( \tilde{E} \) and \( P, Q \) are defined over \( \mathbb{Q} \).

This will be proved in §7.3 when we introduce Hecke operator.
Chapter 7
Hecke operators

In this chapter we introduce one of the fundamental features of modular forms which is responsible for many arithmetic properties. This is namely the Hecke operators acting on the space of modular forms. There are many text books covering this topic perfectly, see for instance Apostol’s book [Apo90] Chapter 6. We will adopt a more geometric approach suitable for the same topic in the context of algebraic geometry of elliptic curves. The first application of Hecke operators is the following.

Theorem 7.0.2 The numbers \( \tau(n) \) are multiplicative, that is for all \( n, m \in \mathbb{N} \) with \( (n, m) = 1 \) we have

\[
\tau(n \cdot m) = \tau(n) \cdot \tau(m)
\]

7.1 Hecke operators

So far, we have interpreted modular forms as functions in three spaces:

1. The Poincaré upper half plan \( \mathbb{H} \),
2. the space \( \mathcal{P} \) of lattices,
3. and the affine space \( \mathbb{A}^2 \mathbb{C} \) with the coordinate system \( (t_2, t_3) \).

In this section for each natural number \( n \) we want to define the Hecke operator

\[
T_n : M_k \to M_k
\]

which is a linear map. It is given by one of the following equivalent definitions:

1. For \( f : \mathbb{H} \to \mathbb{C} \) a modular form of weight \( k \) we have

\[
T_n(f) = \sum_{i=1}^{s} f|_{kA_i},
\]

where \( \{[A_1], [A_2], \cdots [A_s]\} = \text{SL}(2, \mathbb{Z})/\text{Mat}_n(2, \mathbb{Z}) \).
2. For \( f : \mathcal{S} \to \mathbb{C} \) a modular form of weight \( k \) we have
\[
T_n(f)(\Lambda) = n^{k-1} \sum_{\Lambda'} f(\Lambda'),
\]
where \( \Lambda' \) runs through all sublattices \( \Lambda' \subset \Lambda \) of index \( n \). This means that \( \#(\Lambda/\Lambda') = n \).

3. For \( f \) a homogeneous polynomial of degree \( k \) in \( \mathbb{C}[t_2,t_3] \), \( \deg(t_2) = 4 \), \( \deg(t_3) = 6 \) we have
\[
T_n(f)(t_2,t_3) = n^{k-1} \sum_{t'} f(t'),
\]
where \( t' = (t'_2, t'_3) \) runs through all parameters for which there is an isogeny \( \alpha : E_{t'} \to E_t \) such that \( \alpha^*(\frac{dt}{y}) = \frac{dt}{y} \) and \( \deg(\alpha) = n \).

**Exercise 41** Prove the equivalence of the above definitions.

**Exercise 42** Prove that each equivalence class in \( \text{SL}(2,\mathbb{Z})/\text{Mat}_n(2,\mathbb{Z}) \) is represented exactly by one of the matrices
\[
\begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix}, \quad d|n, \ 0 \leq b < \frac{n}{d}.
\]

Using the above exercise we know that the action of the Hecke operator \( T_n \) on a modular form of weight \( k \) defined on the upper half plane is given by
\[
T_n(f)(\tau) = n^{k-1} \sum_{a-d=n, \ 0 \leq b \leq d-1} d^{-k} f\left(\frac{a\tau+b}{d}\right) \tag{7.1}
\]

**Proposition 7.1.1** For two natural numbers \( n, m \) and Hecke operators \( T_n, T_m \in \text{Mat}_k \) prove that
\[
T_n \circ T_m = \sum_{d|(n,m)} d^{k-1} \frac{T_{nm}}{d^2}. \tag{7.2}
\]

In particular, for \( n \) and \( m \) coprime we have
\[
T_n \circ T_m = T_{nm}
\]
and for \( p \) a prime number
\[
T_p \circ T_p = T_p^{p+1} + p^{k-1} T_{p^{k-1}}. \tag{7.3}
\]

**Proof.** We follow [Silvermann] page 69. The idea of the proof is more and less in [Silvermann I] page 62. Let \( n, m \in \mathbb{N} \) and \( d|(n,m) \) be fixed. We prove that for pairs of isogenies,
\[
E_1 \xrightarrow{\alpha} E_2 \xrightarrow{\beta} E, \quad \deg \alpha = n, \ \deg \beta = m
\]

There is a unique isogeny \( E_1 \xrightarrow{\varphi} E \), \( \deg \varphi = \frac{mn}{d^2} \) such that
and for \( h \) fixed we have \( d \) pairs of such isogenies \( \alpha, \beta \).

This decomposition is inspired by the identity

\[
\sigma(n) \cdot \sigma(m) = \sum_{d \mid (n,m)} d \cdot \sigma \left( \frac{nm}{d^2} \right)
\]

If this is the case, then

\[
T_n \circ T_m f(\mathcal{E}, \omega) = (n,m)^{k-1} \sum_{E_1 \alpha, E_2 \beta \mathcal{E}} f \left( E_1, (\beta \circ \alpha)^* \omega \right)
\]

\[
= \sum_{d \mid (n,m)} (nm)^{k-1} d \sum_{E_1 \alpha, E_2 \beta \mathcal{E}} f \left( E_1, (\beta \circ \alpha)^* \omega \right)
\]

\[
= \sum_{d \mid (n,m)} (nm)^{k-1} d^{k-1} f(\mathcal{E}, \omega)
\]

\[
= \sum_{d \mid (n,m)} d^{k-1} T \frac{nm}{d^2}
\]

we have used \([d]^* \omega = d \omega\) and \(f(\mathcal{E}, d^*) = d^{-k} f(\mathcal{E}, \star)\)

in the order to prove the affirmation on isogenies we prove the corresponding affirmation on lattices. Let \( \Lambda \subseteq \mathbb{C} \) be a fixed lattices and

\[
\Lambda_1 \subseteq \Lambda_2 \subseteq \Lambda \quad \# \frac{\Lambda_2}{\Lambda_1} = n, \quad \# \frac{\Lambda}{\Lambda_2} = m
\]

For \((n,m) = 1\), \( \Lambda_2 \) is uniquely characterized by

\[
\Lambda_2 = \{ x \in \Lambda \mid nx \in \Lambda_1 \}
\]

and the affirmation is trivial. We fin a subgroup

\[
G_d := \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \subseteq \Lambda / \Lambda_1
\]

and define

\[
\Lambda_3 = \text{pull-back of } G_d \text{ by } \Lambda \to \Lambda / \Lambda_1
\]

We have

\[
d \Lambda_3 \subseteq \Lambda_1 \subseteq \Lambda_3
\]

and the index in both inclusions \( d \Lambda_3 \subseteq \Lambda_3 \) and \( \Lambda_1 \subseteq \Lambda_3 \) is \( d^2 \). Therefore \( \Lambda_3 = \Lambda_1 \).

We have to show that there are \( d \) such \( G_d \) and hence \( \Lambda_3 \).

\( \square \)

The formula (??) is summarized in the following formal equality:
\[ \sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p}(1 - T_p p^{-s} + p^{k-1-2s})^{-1} \]

Let \( f \) be a modular form with the Fourier expansion:
\[ f(z) = \sum_{n=0}^{\infty} a_n q^n, \quad q = e^{2i\pi z}. \]

For \( m \in \mathbb{N} \), we have \( T_m f(z) = \sum_{n=0}^{\infty} b_n q^n \), where
\[ b_n = \sum_{d | \text{gcd}(m, n)} d^{k-1} a_{mn/d^2}. \]

**Exercise 43** Can you show by algebraic geometric methods that for fixed \( t \in \mathbb{C}^2 \setminus \{ \Delta = 0 \} \) the set of parameters \( t' \) with
\[ \alpha : E_t' \to E_t, \quad \alpha^* \frac{dx}{y} = \frac{dx}{y}, \quad \deg(\alpha) = n \]

is finite.

Let \( A \) be an element in the group generated by \( \text{GL}_+(2, \mathbb{R}) \) and \( \{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{C}^* \} \cong \mathbb{C}^* \). Let also \( \omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathcal{P} \). Then
\[ A \omega \in \mathcal{P}. \]

Using the map \( \phi \) in Weierstrass uniformization theorem, we can translate the above process to the \((t_2, t_3)\)-space. Namely, for each \( t \in \mathbb{C}^2 \setminus \{ \Delta = 0 \} \) and a basis of the homology \( \delta_1, \delta_2 \in H_1(E_t, \mathbb{Z}) \) with \( \langle \delta_1, \delta_2 \rangle = 1 \) and \( A \) as above we have a local holomorphic map \( t \mapsto \alpha(t) \). If we choose another basis of \( H_1(E_t, \mathbb{Z}) \) obtained by the previous one by an element \( B \in \text{SL}(2, \mathbb{Z}) \), then we have a new period matrix \( AB \omega \).
This is equal to \( A \omega \) in \( \mathcal{P} \) if and only if
\[ ABA^{-1} \in \text{SL}(2, \mathbb{Z}). \]

We conclude that if we choose representatives for the quotient
\[ (A \cdot \text{SL}(2, \mathbb{Z}) \cdot A^{-1} \cap \text{SL}(2, \mathbb{Z})) \setminus (A \cdot \text{SL}(2, \mathbb{Z}) \cdot A^{-1}) = \{ [A_i] \mid i = 1, 2, \ldots, s \} \]
then to each \( A_i \) we have associated a local map \( \alpha_i(t) \).

**Exercise 44** Let \( A_i = AS_iA^{-1}, \quad S_i \in \text{SL}(2, \mathbb{Z}) \). Show that
\[ \text{SL}(2, \mathbb{Z})/\text{Mat}_n(2, \mathbb{Z}) = \{ [AS_i] \mid i = 1, 2, \ldots, s \} \]
and vice-versa.
Exercise 45 Let \( n \in \mathbb{N} \). Are there polynomials \( p_n, i = 2, 3 \) such that \( p_n(z) = (p_{n,2}, p_{n,3}) \) leaves \( \Delta = 0 \) invariant and

\[
T_n(f)(t) = f(p_n^{-1}(t)), \quad f \in \mathcal{M}_k,
\]

where \( f(X) = \sum_{x \in X} f(x) \).

7.2 Hecke and cusp forms

Theorem 7.2.1 Let \( f \) be a cusp form of weight \( k \) and suppose that \( f \) is an eigenform for all Hecke operators and \( f_n = 1 \). Then

\[
T_n f = f_n \cdot f
\]

Proof. We have \( T_n f = \lambda_n \cdot f \) and so

\[
\lambda_n f_m = (T_n f)_m = \sum_{d|\gcd(n,m)} d^{k-1} \frac{f_m}{d^2}
\]

We put \( m = 1 \) and get \( \lambda_n = f_n \)

Definition 7.2.1 A normalized eigen function is a modular form \( f \) with 1. \( f \) is a cusp form with \( f_1 = 1 \) 2. \( T_n f = f_n \cdot f \)

Exercise 46 (1.25 Silvermann II page 92) 1. \( E_k \) is an eigenform for all Hecke operators. 2. if \( f \) is an eigen form for all Hecke operators and \( f \) is not a cusp form then \( f \) is a multiple of \( E_k \)

Theorem 7.2.2 Let \( f(\tau) = \sum_{n=1}^{\infty} f_n \tau^n \) be a normalized eigen function of weight \( k \). Then

\[
f_n m = f_n m \quad (n,m) = 1 \quad f_{p^r} \cdot f_p = f_{p^{r+1}} + p^{k-1} f_{p^{r-1}} \quad \text{p prime}
\]

Proof. \( T_n f = f_n \cdot f \) and the theorem follows from [taken from Silvermann page 79]

Our main example is

\[
\Delta = q \tau(1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n
\]

We have

\[
\tau(n) \tau(m) = \tau(nm) \quad (n,m) = 1 \quad \tau(p) \tau(p^n) = \tau(p^{n+1}) + p^{11} \tau(p^{n-1}) \quad (7.4)
\]

This follows from the fact that \( S_{12} \left( \text{SL}(2, \mathbb{Z}) \right) \) is generated by \( \Delta \)

The identities were conjectured by Ramanujan and proved by Mordell.

Exercise 47 Can you find a basis of \( S_n \left( \text{SL}(2, \mathbb{Z}) \right) \), \( n = 14, 16, 18 \) which are normalized eigen forms
7.3 Proof of Theorem 6.3.1

First we prove that $\tilde{E}$ is defined over $\mathbb{Q}$.

In order to see the analogy between holomorphic and algebraic context we define
$$
(x,y) = \left( \wp(z,\Lambda), \wp'(z,\Lambda) \right)
$$
$$
(\tilde{x},\tilde{y}) = \left( \wp(z,\tilde{\Lambda}), \wp'(z,\tilde{\Lambda}) \right)
$$

$f^{-1}(O)$ and $f^{-1}(P)$ both contains $N$ points and let

$$
\tilde{x}\left(f^{-1}(O)\right) = \{\infty,a_2,a_3,\ldots,a_s\} \subseteq \mathbb{Q}
$$
$$
\tilde{x}\left(f^{-1}(P_1)\right) = \{b_1,b_2,\ldots,b_r\} \subseteq \mathbb{Q}
$$

(7.5)

Since $\tilde{E}$ is defined over $\mathbb{Q}$ its torsion points are also defined over $\mathbb{Q}$ and the inclusions $\mathbb{Q}$ above follows. There is no repetition among $a_i$'s (resp. $b_i$'s). Note that the map $\tilde{E} \to \tilde{E}$, $X \to -X$ leaves both sets $f^{-1}(O)$ and $f^{-1}(P_1)$ invariant. For $f^{-1}(P_1)$ this follows from $P_1 = -P_1$. Moreover

$$
\tilde{x}(x) = \tilde{x}(-x), \ X \in \tilde{E}
$$

It follows that $s = r$. Analysing the set of poles and zeros of $(x-e_1)$ of we get

$$
(x-e_1) of = a \prod_{i=1}^{r}(\tilde{x}-b_i) \prod_{i=2}^{s}(\tilde{x}-a_i)
$$

For some $a \in \mathbb{C}$. Since $f$ sends torsions of $\tilde{E}$ to $E$ evaluating $(x-e_1) of$ at any torsion points of $\tilde{E}$ different from $7.5$ we get $a \in \mathbb{Q}$. □

In a similar way, we have

$$
\frac{y of}{\tilde{y}} = \frac{\prod(\tilde{x}-c_i)}{\prod(\tilde{x}-d_i)}
$$

Where $c_i, d_i$'s are algebraic numbers obtained by evaluating $\tilde{x}$ at $f^{-1}(E[2])$.

Let $f \in M_k$ be modular form defined over $\mathbb{Q}$.

$$
P(x) = \prod \left( x - f(\tilde{\Lambda}) \right)
$$

$$
\tilde{\Lambda} \subseteq \Lambda, \quad \#\Lambda/\tilde{\Lambda} = n
$$
The coefficients of $P(x)$ are symmetric polynomials in $N = \sigma(n)$ quantities $\sum_{i=1}^{N} x_i, \sum_{i<j} x_i x_j, \sum_{i<j<k} x_i x_j x_k, \ldots$

We can write these as polynomials with coefficients in $\mathbb{Q}$ of the quantities $\sum_{i=1}^{N} x_i^m, \quad m = 1, 2, 3, \ldots$

These are $T_n f^m$. It is enough to prove that Hecke operators send modular forms defined over $\mathbb{Q}$ to modular forms defined over $\mathbb{Q}$. This follows from the computation of q-expansion of $\langle T_n f \rangle$.

We know that $f$ sends $\overline{E}(\Omega)_{\text{tors}}$ to $E(\Omega)_{\text{tors}}$, therefore for an elliptic function $P$ on $E$ with poles and zeros on torsion points of $E$, the pull-back of $P$ by $f$ has poles and zeros in torsion points of $\overline{E}$.

We write $\wp'_{\Lambda}(z, \Lambda)^2 = 4 \left( \wp(z, \Lambda) - e_1 \right) \left( \wp(z, \Lambda) - e_2 \right) \left( \wp(z, \Lambda) - e_3 \right)$

$\wp(z, \Lambda) - e_1$ has a pole of order two at $O$ and a zero of multiplicity 2 at a 2-torsion point. The pull-back of this function gives us the desired result.
Chapter 8
Riemann zeta function

In this chapter we introduce the Riemann zeta function. We will follow mainly the Riemann’s original article ([Rie]) and the book [Edw01] which explain an historical account on Riemann’s paper. Euler considered the zeta function

\[ \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \]

for real \( s \) and Riemann introduced \( \zeta(s) \) for complex \( s \) and its extension as a meromorphic function to the whole \( s \)-plane. In particular, it was known before Riemann that

\[ \zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450} \]

8.1 Riemann zeta function

In this section we are going to study the first of all Zeta function, namely Riemann zeta function:

\[ \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \]

We mainly use the Riemann’s original article [Rie].

**Proposition 8.1.1** The series \( \zeta(s) \) converges for all \( s \in \mathbb{C} \) with \( \Re(s) > 1 \) and

\[ \zeta(s) = \prod_p \frac{1}{1 - p^{-s}}. \]

where \( p \) runs over all primes.

**Proof.** We have \( |n^{-s}| = n^{\Re s} \) and so it is enough to prove the proposition for \( s \in \mathbb{R}, s > 1 \). We have
\[
\sum_{n=2}^{\infty} \frac{1}{n^2} \leq \int_1^{\infty} x^{-s} \, dx = \frac{x^{-s+1}}{-s+1} \bigg|_{1}^{\infty} = \frac{1}{s-1} \text{ if } s > 1
\]

Again we assume that \( s \) is a real number bigger than 1. We have \( p^{-s} < 1 \) and so

\[
(1 - p^{-s}) = \sum_{m=0}^{\infty} p^{-ms}.
\]

By unique factorization theorem

\[
\prod_{p \leq N} (1 - p^{-s})^{-1} = \sum_{n \leq N} n^{-s} + R_N(s).
\]

Clearly

\[
R_N(s) \leq \sum_{n=N+1}^{\infty} n^{-s}.
\]

Since \( \zeta(s) \) converges we have \( R_N(s) \to 0 \) as \( N \to \infty \) and the result follows.

### 8.2 The big Oh notation

In this section for \( a \in \mathbb{R} \cup \{-\infty\} \) we define the interval \( I_a \) to be a small one sided neighborhood of \( a \). If \( a \in \mathbb{R} \) this means that \( I_a = (a, a + \varepsilon) \) or \( (a - \varepsilon, a) \) for some small \( \varepsilon \) and for \( a = +\infty \) this means \( I_a = (b, +\infty) \) for a big positive number \( b \) and for \( a = -\infty \) this means \( I_a = (-\infty, -b) \) for a big positive number \( b \).

**Definition 8.2.1** Let \( f, g \) be two complex valued function in \( I_a \) we write

\[
f = O(g) \text{ or } f \sim_{x \to a} g
\]

to say that \( \frac{f(x)}{g(x)} \) is bounded near \( a \), that is there exists a constant \( M \) such that

\[
|f(x)| \leq M |g(x)|, \forall x \in I_a.
\]

For three complex valued functions \( f, g \) and \( h \) in \( I_a \) we write \( f(x) = h(x) + O(g(x)) \) if \( f(x) - h(x) = O(g(x)) \).

We mainly use the following convergence criterion: Let \( f \) be a complex valued continuous function in \( I_a, a \in \mathbb{R} \) and

\[
f \sim_{x \to a} (x - a)^s, \quad s \in \mathbb{R}.
\]

For \( a = \pm \infty \) we assume \( f \sim_{x \to a} x^s \), We can extend this assumption to \( s = \pm \infty \). For instance for \( a \in \mathbb{R} \) the expression \( f \sim_{x \to a} (x - a)^{+\infty} \) means

\[
\forall s \in \mathbb{R}^+, \quad f \sim_{x \to a} (x - a)^s
\]
For \(a, s \in \mathbb{R}\) the integral 
\[
\int_{a}^{\infty} f(x)\,dx
\]
converges if \(s > -1\). If \(a = \pm \infty, s \in \mathbb{R}\) then the integral \(\int_{a}^{\infty} f(x)\,dx\) converges if \(s < -1\).

### 8.3 Gamma function

The gamma function is defined by
\[
\Gamma(s) = \int_{0}^{\infty} x^{s-1}e^{-x}\,dx, \quad \Re(s) > 0
\]
It converges because near 0
\[
x^{s-1}e^{-x} \sim_{x \to 0} x^{\Re(s) - 1}
\]
and so for \(\Re(s) > 0\) the integral near zero converges. Near infinity it is always convergent because
\[
x^{s-1}e^{-x} \sim_{x \to +\infty} x^{-n-1}, \quad \forall n \in \mathbb{N}.
\]
We have
\[
\Gamma(s) = (s - 1)\Gamma(s - 1)
\]
(8.1)
because
\[
\Gamma(s) = -\int_{0}^{\infty} x^{s-1}dxe^{-x} = \cdots = (s - 1)\Gamma(s - 1)
\]
Since \(\Gamma(1) = 1\) this implies that
\[
\Gamma(n) = (n - 1)!, \quad n \in \mathbb{N}
\]
and so the \(\Gamma\)-function is the interpolation of the factorial function.

The equalities
\[
\Gamma(s) = \frac{\Gamma(s + 1)}{s} = \cdots = \frac{\Gamma(s + n + 1)}{s(s + 1)\cdots(s + n)}, \quad n \in \mathbb{N}
\]
enables us to continue \(\Gamma\) analytically onto all of the complex \(s\)-plane with poles of simple order at \(s = 0, -1, -2, \ldots\). We have also Euler’s reflection formula
\[
\Gamma(1-s)\Gamma(s) = \frac{\pi}{\sin(\pi s)}
\]
(8.2)
which shows that \(\Gamma\) has no zeros. We have also the equality
\[
\Gamma(s) \Gamma\left(s + \frac{1}{2}\right) = 2^{1-2s} \sqrt{\pi} \Gamma(2s).
\]

**Remark 8.3.1** Gauss introduced the notation \(\Pi(s) = \Gamma(s + 1)\) which is used in Riemann’s original article. The notation \(\Gamma\) is due to Legendre, see [Edw01] p. 8.

### 8.4 Mellin transform

The content of this section is taken from Wikipedia. The Mellin transform of a function \(f\) defined on \(\mathbb{R}^+\) is

\[
\int_0^\infty x^s f(x) \frac{dx}{x}.
\]

If \(f(x)\) is locally integrable along the positive real line, and

\[
f(x)_{x \to 0^+} = O(x^u) \quad \text{and} \quad f(x)_{x \to +\infty} = O(x^v)
\]

then its Mellin transform converges in the fundamental strip \([-u, -v]\).

By definition the \(\Gamma\) function is the Mellin transform of \(e^{-x}\).

### 8.5 Analytic extension

From the definition of \(\Gamma\)-function it follows:

\[
\frac{\Gamma(s)}{n^s} = \int_0^\infty x^{s-1} e^{-nx} dx, \quad \Re(s) > 1 \quad (8.3)
\]

Taking sum for \(n = 1, 2, \ldots\) we obtain

\[
\Gamma(s) \zeta(s) = \int_0^\infty x^{s-1} \frac{dx}{e^x - 1}, \quad \Re(s) > 1.
\]

One can see that near \(+\infty\) we have \(\frac{1}{e^x - 1} = O(x^{-\infty})\) and near 0 we have \(\frac{1}{e^x - 1} = O(x^{-1})\). Therefore, the convergence strip for the above integral is \(\Re(s) \in (1, +\infty)\) (see the section on Mellin transform).

Now, we consider the integral

\[
I(s) := \int_{+\infty}^{+\infty} \frac{(-x)^s}{e^x - 1} \frac{dx}{x}
\]

Here, we have taken the branch of \((-x)^s = e^{s \ln(-x)}\) in \(\mathbb{C}\setminus\mathbb{R}^+\) such that \(\ln(-x)\) for negative \(x\) is a real number. The path of integration begins at \(+\infty\), moves to the left up to the positive axis, circles the origin once in the counterclockwise direction, and returns down to the positive real axis to \(+\infty\). Now the above integral is convergent.
8.6 Functional equation

for all \( s \) and it gives an entire function in \( s \). A simple calculation show that it is equal to

\[
I(s) = (e^{\pi i s} - e^{-\pi i s}) \int_0^\infty \frac{x^s}{e^x - 1} \, dx, \quad \Re(s) > 1
\]

In particular, this shows that \( I(s) \) vanishes in \( s = 2, 3, \ldots \). Therefore, we get

\[
2i \sin(\pi s) \Gamma(s) \zeta(s) = \int_{+\infty}^{+\infty} \frac{(-x)^s}{e^x - 1} \, dx
\]

and by (8.2)

\[
\zeta(s) = \frac{\Gamma(1-s)}{2\pi i} \int_{|x| = \varepsilon} \frac{(-x)^s}{e^x - 1} \, dx
\]

This equality shows that

1. \( \zeta(s) \) extends to a meromorphic function on the \( s \) plane
2. it has a unique pole in \( s = 1 \). The point \( s = 1 \) is a simple pole of \( \zeta \).
3. It vanishes in \( s = -2, -4, -6, \ldots \).

The third item follows from the following: The Bernoulli numbers \( B_k \) are given by

\[
\frac{x}{e^x - 1} = \sum_{k=1}^\infty \frac{B_k}{k!} x^k = 1 + \frac{x}{1!} + \frac{1}{2!} x^2 + \frac{1}{3!} x^3 + \frac{1}{4!} x^4 + \frac{1}{6!} x^6 + \frac{1}{8!} x^8 + \frac{5}{10!} x^{10} + \cdots
\]

For \( s \in \mathbb{Z}, s \leq 0 \) we have

\[
\zeta(s) = -\frac{\Gamma(1-s)}{2\pi i} \int_{|x| = \varepsilon} \frac{(-1)^s - 1}{m!} \left( \sum_{m=0}^\infty (-1)^s B_m x^m + s - 2 \right) \, dx = -\Gamma(1-s)(-1)^{s-1} \frac{B_{1-s}}{(1-s)!}
\]

8.6 Functional equation

By Cauchy theorem for \( s \) with \( \Re(s) < 0 \) we get

\[
2\sin(\pi s) \Gamma(s) \zeta(s) = (2\pi i)^s((-i)^{s-1} + i^{s-1}) \sum_{n=1}^\infty n^{s-1}
\]

In other words the function

\[
\Gamma\left(\frac{s}{2}\right) \pi^{-\frac{s}{2}} \zeta(s)
\]

remains invariant under \( s \mapsto 1 - s \). By analytic continuation this holds in the whole \( s \)-plane.

**Exercise 48** Find the values of \( \zeta \) for even positive integers:

\[
\zeta(2n) = \frac{(2\pi)^{2n}(-1)^{n+1}B_{2n}}{2 \cdot (2n)!}
\]
8.7 Second proof for functional equation

In the equality (8.3) we make the change of variables \( n \to n^2 \pi \) and \( s \to \frac{s}{2} \) and we obtain:
\[
\frac{\Gamma\left(\frac{s}{2}\right)}{n^s} \pi^{-\frac{1}{2}} = \int_0^\infty x^{\frac{s}{2}-1} e^{-n^2 \pi x} dx, \quad \Re(s) > 1
\]
Define
\[
\psi(x) := \sum_{n=1}^\infty e^{-n^2 \pi x}
\]
and so
\[
\zeta(s) \Gamma\left(\frac{s}{2}\right) \pi^{-\frac{1}{2}} = \int_0^\infty x^{\frac{s}{2}-1} \psi(x) dx, \quad \Re(s) > 1
\]  
(8.4)

Exercise 49 Prove that \( \psi \) converges and
\[
1 + 2 \psi(x) = x^{-\frac{1}{2}} (1 + 2 \psi\left(\frac{1}{x}\right)). \tag{8.5}
\]
Moreover, the above integral converges for \( \Re(s) > 1 \). We have the theta series
\[
\theta_3(z) := \sum_{n=-\infty}^{\infty} q^{\frac{1}{2} n^2}, \quad q = e^{2\pi i z}, \quad z \in \mathbb{H}
\]
which is related to \( \psi \) by
\[
\theta_3(z) = 1 + 2 \psi(-iz).
\]
Using (8.5) one can see that
\[
\zeta(s) \Gamma\left(\frac{s}{2}\right) \pi^{-\frac{1}{2}} = \int_1^\infty \left( x^{\frac{s}{2}} + x^{\frac{1-s}{2}} \right) \psi(x) \frac{dx}{x} \frac{1}{s(1-s)}, \quad s \in \mathbb{C}
\]  
(8.6)
for which the right hand side is convergent for all \( s \in \mathbb{C} \). We multiply the above equality by \( \frac{d(s-1)}{ds} \) and define
\[
\xi(s) := \Gamma\left(\frac{s}{2} + 1\right)(s-1)\pi^{-\frac{1}{2}} \zeta(s)
\]
which is an entire function and satisfies \( \xi(s) = \xi(1-s) \).

Exercise 50 From (8.4) we have
\[
i^\frac{s}{2} \zeta(s) \Gamma\left(\frac{s}{2}\right) \pi^{-\frac{1}{2}} = \int_0^\infty z^{\frac{s}{2}-1} \psi(-iz) dz, \quad \Re(s) > 1
\]
In the above formula, use the Schwarz map of the family of elliptic curves \( y^2 - x^3 + 3x - t = 0 \) and write \( \zeta \) as an integral in the \( t \)-domain. For this you have to calculate
\[ \psi \left( \frac{\log \frac{d}{d\log y}}{\log \frac{1}{1-y}} \right) \text{ as a polynomial in elliptic integrals. In particular, one may prove in this way that } \zeta(s) \text{ for } s \text{ integer is a period.} \]

### 8.8 Zeta and primes

In this section we sketch the relation between primes and the zeros of \( \zeta \).

**Theorem 8.8.1** The sum

\[
\sum_{\rho} (\ln(1 - \frac{s}{\rho}) + \ln(1 - \frac{s}{1-\rho}))
\]

where \( \rho \) runs over all roots of \( \xi \) with \( \text{Im}(\rho) > 0 \), converges absolutely. In particular,

\[
\zeta(s) = \xi(0) \prod_{\rho} (1 - \frac{s}{\rho}).
\]

where the infinite product is taken in an order which pairs each root \( \rho \) with \( 1 - \rho \).

We have

\[
\ln \zeta(s) = \sum_{p} \sum_{n} \frac{1}{n} p^{-ns} = s \int_{0}^{\infty} J(x)x^{-s-1}dx, \quad \Re(s) > 1 \tag{8.7}
\]

where

\[
J(x) := \frac{1}{2} \left( \sum_{p^n \leq x} \frac{1}{n} + \sum_{p^n \leq x} \frac{1}{n} \right).
\]

The order of summation in (8.7) is unimportant because it is absolutely convergent. Now we use the Fourier inversion

\[
J(x) = \frac{1}{2\pi i} \int_{a+i\infty}^{a-i\infty} \ln \zeta(s)x^{s} \frac{ds}{s}, \quad a > 1 \tag{8.8}
\]

we have also

\[
\ln(\zeta(s)) = \ln(\xi(0)) + \sum_{\rho} \ln(1 - \frac{s}{\rho}) - \ln\Gamma\left(\frac{s}{2} + 1\right) + \frac{s}{2} \ln \pi - \ln(s-1). \tag{8.9}
\]

The direct substitution of (8.9) in (8.8) leads to divergent integrals. For this reason we write

\[
J(x) = \frac{1}{2\pi i \ln(x)} \int_{a+i\infty}^{a-i\infty} \frac{d}{ds} \left( \frac{\ln \zeta(s)}{s} \right)x^{s} ds, \quad a > 1 \tag{8.10}
\]

Now the substitution of (8.9) gives us convergent integrals and a formula for \( J(x) \):

\[
J(x) = \text{Li}(x) - \sum_{\text{Im}(\rho) > 0} (\text{Li}(x^{\rho}) + \ln(x^{1-\rho})) + \int_{x}^{\infty} \frac{dt}{t(t^{2}-1)\ln(t)} + \ln(\xi(0)), \quad x > 1,
\]
where
\[ \text{Li}(x) := \int_0^x \frac{dt}{\ln(t)}. \]

Now we derive a formula for
\[ \pi(x) = \sum_{p \leq x} 1 \]
using
\[ \pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} J(x^{\frac{1}{n}}), \]
where \( \mu(n) \) is zero if \( n \) is divisible by a prime square, 1 if \( n \) is a product of an even number of distinct primes, and \(-1\) otherwise.

### 8.9 Other zeta functions

There are many generalizations of the Riemann Zeta function. One of them is already used in §10.2. Below we explain how the zeta functions of a curve over a finite field is a generalization of the Riemann zeta function.

Consider a plane affine curve \( C : f(x,y) = 0, \ f \in \mathbb{F}_p(x,y) \) defined over the field \( \mathbb{F}_p \). In analogy with the Riemann zeta function we define
\[
\zeta(C,s) = \prod_p \frac{1}{1 - (Np)^{-s}}.
\]
(8.11)
where \( p \) runs over all non-zero prime ideals of \( \mathbb{F}_p[C] := \mathbb{F}_p[x,y]/ \langle f(x,y) \rangle \). Here \( Np \) is the order of the quotient \( \mathbb{F}_p[C]/p \). Since such a quotient is a finite integral domain it is a field and hence it has \( p^n \) elements. We define \( \deg(p) := n \). This allows us to redefine the zeta function as follows:
\[
Z(C,T) = \prod_p \frac{1}{1 - T^{\deg(p)}}.
\]
with \( \zeta(C,s) = Z(C,p^{-s}) \).

**Proposition 8.9.1** Let \( C \) be a curve over the finite field \( \mathbb{F}_p \). We have
\[
Z(C,T) = \exp\left( \sum_{r=1}^{\infty} \frac{\#C(\mathbb{F}_p^r)}{r} T^r \right)
\]
For a proof see [Mil96] p. 90.

**Exercise 51** Calculate the zeta functions of \( A^1 \) and \( \mathbb{P}^1 \).

**Exercise 52** Calculate the zeta function of degenerated elliptic curves:
\[ y^2 = x^3 + ax + b, \ 4a^3 + 27b^2 = 0. \]
8.10 Dedekind Zeta function

In this section we give a summary of Dedekind Zeta functions. Let $k$ be a number field and $\mathcal{O}_k$ be its ring of integers.

**Theorem 8.10.1** The integer ring of a number field is a Dedekind domain, i.e every ideal $a \subset \mathcal{O}_k$ in a unique way can be written

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

where $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and $p_1, \ldots, p_s$ are prime ideals.

A character $\chi$ on $\mathcal{O}_k$ is a map from the set of non-zero ideals of $\mathcal{O}_k$ to $\mathbb{C}$ such that it is multiplicative:

$$\chi(a_1 a_2) = \chi(a_1) \chi(a_2).$$

We mainly use the Character $\chi \equiv 1$. Formally, the Dedekind Zeta function is defined in the following way:

$$\zeta_k(s) = \sum_a \frac{\chi(a)}{N(a)^s} = \prod_p \frac{1}{1 - \chi(p) N(p)^{-s}}, \quad N(a) = #(\mathcal{O}_k/a),$$

where the sum is running in non-zero ideals of $\mathcal{O}_k$ and the product is running in the prime ideals of $\mathcal{O}_k$.

**Exercise 53** Discuss the convergence of the Dedekind Zeta function (put $\chi \equiv 1$).

**Exercise 54** Discuss the fact that the integer ring of a number field is not necessarily a unique factorization domain/principal ideal domain. Give examples of irreducible but not prime elements. Hint $\mathbb{Q}(\sqrt{-5})$

$$2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

$$\langle 6 \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle$$

**Exercise 55** The ring of Gaussian integers is $\mathbb{Z}[i]$. Prove that the prime ideals of $\mathbb{Z}[i]$ are of two types:

$$p = \langle p \rangle, \quad \text{if } p \equiv 3(4), \quad = \langle a + ib \rangle, \quad \text{if } a^2 = b^2 = p \equiv 1(4).$$

In the second case we say that $p$ splits in $\mathbb{Z}[i]$. Show that the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Show also that the only ideal which ramifies is $p = \langle 1 + i \rangle$, i.e. $p^2 = \langle p \rangle$.

8.11 L-function of cusp forms

We follow [Silvermann II] page 80-84

We first define L-functions for the full modular group.
Let \( f = \sum_{n=1}^{\infty} f_n q^n \) \( f_1 = 1 \), be a normalized eigenfunction of weight \( k \). Then

\[
f_{mn} = f_m f_n \quad (n,m) = 1 \\
f_{p^e} f_p = f_{p^{e+1}} + p^{k-1} f_{p^{e-1}} \quad e \geq 1
\]

**Proposition 8.11.1** We have

\[
L(f, s) := \sum_{n=1}^{\infty} \frac{f_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-f_p p^{-s} + p^{k-1-2s}}
\]

for \( \text{Re}(s) > \frac{k}{2} + 1 \)

**Proof.** The convergence follows from \( f_n \sim n^k \) and the same convergence statement for Riemann’s zeta function

\[
L(f, s) = \sum_{n} f_n \cdot n^{-s} = \prod_{\text{p prime}} \sum_{e \geq 0} f_{p^e} \cdot p^{-es}
\]

we have

\[
(1 - f_p p^{-s} + p^{k-1-2s}) \left( \sum_{e \geq 0} f_{p^e} \cdot p^{-es} \right) = \sum_{e \geq 0} f_{p^e} p^{-es} - \sum_{e \geq 0} f_{p^e} \cdot f_p p^{-s-es} + \sum_{e \geq 0} f_{p^e} p^{k-1-2s-es} \]

\[
= A + C - \sum_{e \geq 1} (f_{p^e} + p^{k-1} f_{p^{e-1}} p^{-s-es} - f_p \cdot p^{-s})
\]

\[
= A + C - (A - f_p p^{-s}) - C - f_p p^{-s} = 1
\]

The product in (8.12) is also called the Euler product of L-function.

**Theorem 8.11.1 (Hecke):** Let \( f \) be a cusp form of weight \( k \) for \( SL(2, \mathbb{Z}) \) Then

1. \( L(f, s) \) has an analytic extension to \( \mathbb{C} \)
2. \( R(f, s) := (2\pi)^{-s} \Gamma(s)(f, s) \). Then \( R(f, k-s) = (-1)^{\frac{k}{2}} R(f, s) \)

Note that \( R \) is symmetric with respect to \( \text{Re}(s) = \frac{k}{2} \)

We prove this theorem in a general context introduced by Hecke, see (8.12)

### 8.12 Hecke’s L-functions

The following is due to [Hecke1936]. Let us consider a series of the form

\[
f = f_0 + f_1 q^{\lambda^{-1}} + f_2 q^{2\lambda^{-1}} + \ldots + f_n q^{n\lambda^{-1}} + \ldots
\]
Where \( f_i \in \mathbb{C} \) and \( \lambda \in \mathbb{R}^+ \), we assume that \( f \) is convergent in the unit disk and hence if we set \( q = e^{2\pi i \tau} \) then it defines a holomorphic function

\[
    f : \mathbb{H} \rightarrow \mathbb{C}
\]

We further assume that \( f \) satisfies

\[
    f\left( \frac{-1}{\tau} \right) = \gamma \cdot (-i)^k f(\tau)
\]

for some \( \gamma = \pm 1 \) and \( k \in \mathbb{Q} \).

The L-function attached to \( f \) is

\[
    L(f, s) = \sum_{n=1}^{\infty} \frac{f_n}{n^s}
\]

which converges in the region \( \text{Re}(s) > a \) if we assume that \( f_n \sim n^a \). We have

\[
    \frac{\Gamma(s)}{n^s} = \int_0^{\infty} x^{s-1} e^{-nx} \, dx
\]

which implies

\[
    L(f, s) \Gamma(s) = \int_0^{\infty} x^{s-1} \left( \sum_{n=1}^{\infty} f_n \cdot e^{-nx} \right) dx
\]

we make the change of variables \( x \rightarrow 2\pi x \cdot \lambda^{-1} \) and get

\[
    R(f, s) := \frac{L(f, s) \cdot \Gamma(s)}{(2\pi \lambda^{-1})^s} = \int_0^{\infty} x^{s-1} \tilde{f}(\tau) dx, \quad \tau := ix
\]

Where \( f = f_0 + \tilde{f} \). Note that the functional equation of \( \tilde{f} \) is

\[
    \tilde{f}\left( \frac{-1}{\tau} \right) = f_0 \cdot (\gamma x^k - 1) + \gamma x^k \tilde{f}(\tau)
\]

We have

\[
    R(f, s) = \int_0^1 + \int_1^{\infty} = \int_1^{\infty} x^{1-s} \tilde{f}\left( \frac{-1}{\tau} \right) x^{-2} dx + x^{s-1} \tilde{f}(\tau) dx
\]

\[
    = \int_1^{\infty} \gamma x^{-1-s+k} \tilde{f}(\tau) dx + x^{s-1} \tilde{f}(\tau) dx + f_0 \int_1^{\infty} x^{-1-s}(\gamma x^k - 1) dx
\]

\[
    = \int_1^{\infty} \left( \gamma x^{-1-s+k} + x^{s-1} \right) \tilde{f}(\tau) dx + f_0 \cdot \left( \frac{1}{-s - \gamma - k} \right)
\]

We have used \( \text{Re}(s) > k, \text{Re}(s) > 0 \) in order to compute the last integral. The first integral is a holomorphic entire function in \( s \in \mathbb{C} \) and so we conclude that \( R(f, s) \) extends to a meromorphic function in \( s \in \mathbb{C} \) with possible poles at \( s = 0 \) and \( s = k \). Moreover, it satisfies
\[ R(f, k - s) = \gamma R(f, s) \]

Here is the place, where we use \( \gamma = \pm 1 \)

Riemann has used the theta series

\[ \theta_3 = \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}n^2} = 1 + 2 \sum_{n=1}^{\infty} q^{\frac{1}{2}n^2} \]

In this case

\[ \theta_3 \left( \frac{-1}{\tau} \right) = (-i\tau)^{\frac{1}{2}} \theta_3(\tau) \]

and so \( k = \frac{1}{2}, \gamma = +1, \lambda = 2 \). In this case

\[ L(\theta_3, s) = 2 \sum \frac{1}{(n^2)^s} = 2\xi(2s) \]

and so we get the functional equation of \( \xi(s) \)

Note that we could also use Einstein series and define.

\[ L(E_k, s) = \sum_n \frac{\sigma_{k-1}(n)}{n^s} = \sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{d^{s-k} m^s} \]

and so we will get again the functional equation of \( \xi(s) \)

**Exercise 56** Use the functional equation of \( E_2 \)

\[ E_2 \left( \frac{-1}{\tau} \right) = \tau^2 E_2(\tau) + \frac{12}{2\pi i} \tau \]

and describe \( L(E_2, s) \).

### 8.13 L-function of CY-modular forms

The theory of Calabi-Yau forms developed in [Mov17 ?] still lives its infancy. The lack of applications is one the big obstacles for developing the theory further. Looking at the history of (elliptic) modular forms, the author feel himself like E. Hecke who is one of the main resposables for the arithmetic of modular forms, however, he didnt see the most amazing arithmetic applications of modular forms in his life time. In the present text, we would like to develope of L-functions attached to CY-modular forms. Recall the classical L-function attached to a cusp form \( f \).
8.13 L-function of CY-modular forms

\[ L(f, s) = \int_{0}^{\infty} f(\tau) \tau^{s} \cdot \frac{d\tau}{\tau} = \int_{\rho} \]

We regard \( \rho \) as path \( \rho_1 - \rho_2 \), where \( \rho_1 \) connects \( \infty \) to \( i \) and \( \rho_2 \) is

\[ \rho_2 = S \cdot \rho_1, S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \]

Which connects \( i \) to \( O \), in some sense, \( L \) is attached to \( S \) and its fixed point \( i \).

Now, consider \( A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \), with \( A^3 = -I, AP = P \).

Under the iteration of \( A \) we have

\[ i \infty \rightarrow -1 \rightarrow 0 \rightarrow i \infty \]
\[ \tau \rightarrow \frac{\tau + 1}{\tau} \rightarrow \frac{-1}{\tau + 1} \rightarrow \tau \]

Furthermore, we have the functional equations

\[ f \left( \frac{\tau + 1}{\tau} \right) = (-\tau)^k f(\tau), \quad f \left( \frac{-1}{\tau + 1} \right) = (\tau + 1)^k f(\tau) \]

Let \( \delta_1 \) be the path \( \text{Re}(P) \) which connects \( \infty \) to \( P \), \( \delta_2 = A \delta_1 \), \( \delta_3 = A \delta_2 \), see Figure

Let also

\[ \rho_1 = \delta_1 - \delta_2, \rho_2 = \delta_2 - \delta_3, \rho_3 = \delta_3 - \delta_1 \]
\[ L_i := \int_{\rho_i} f(\tau) \tau^{s-1}, \quad i = 1, 2, 3 \] (8.13)

We have

\[ L_1 + L_2 + L_3 = 0 \]

The integrals in (8.13) are convergent at \( \infty, -1, 0 \) respectively.

For \( \tau = it \) we have

\[ |f(it)| \leq M \cdot e^{-2\pi t} \]

and

\[ \lim_{t \rightarrow +\infty} e^{-t} \cdot t^m = 0 \quad \forall m \geq 1 \]

Therefore

\[ \left| \int_{\rho_i} f(\tau) \tau^{s-1} d\tau \right| \leq \left| \int_{\rho} f(it) t^{s-1} dt \right| \leq M \int_{\rho} t^{\text{Re}(s)-1+1} \]
Fig. 8.1 L-function
Chapter 9
Congruence groups

In this chapter we work with modular forms for a congruence subgroup of $\text{SL}(2, \mathbb{Z})$. One of the most well-known applications of such modular forms is the so-called arithmetic modularity theorem.

9.1 Congruence groups

We have seen that $\text{SL}(2, \mathbb{Z})$ appears as the monodromy group of the Weierstrass family of elliptic curves. If we take other families of elliptic curves and compute the corresponding monodromy group then we will get subgroups of $\text{SL}(2, \mathbb{Z})$ of finite index. Congruence groups are the most well-known subgroups of $\text{SL}(2, \mathbb{Z})$. Let $N$ be a positive integer number. Define

$$\Gamma(N) := \left\{ A \in \text{SL}(2, \mathbb{Z}) | A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

It is the kernel of the canonical homomorphism of groups $\text{SL}(2, \mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

**Definition 9.1.1** A subgroup $\Gamma \subset \text{SL}(2, \mathbb{Z})$ is called a congruence subgroup of level $N$ if

1. $\Gamma(N) \subset \Gamma$
2. $A \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} A^{-1} \in \Gamma \quad \forall A \in \text{SL}(2, \mathbb{Z})$

Our main examples are

$$\Gamma_0(N) := \left\{ A \in \text{SL}(2, \mathbb{Z}) | A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_1(N) := \left\{ A \in \text{SL}(2, \mathbb{Z}) | A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$
For a description of a fundamental domain for the action of $\Gamma_0(p)$, $p$ a prime number, see Apostol's book [Apo90] Theorem 4.2.

**Definition 9.1.2** A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of weight $k$ for $\Gamma$ if

1. $f|_A = f$ $\forall A \in \Gamma$
2. For all $A \in \text{SL}(2, \mathbb{Z})$ 
   \[ \lim_{\text{Im}(\tau) \to +\infty} f|_A = \text{exists and } < \infty \]

### 9.2 Weil pairing

Let $\Lambda = \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2 \subset \mathbb{C}$ be a lattice with $\text{Im}(\frac{\omega_1}{\omega_2}) > 0$ and let $E = \mathbb{C}/\Lambda$ be the corresponding elliptic curve. For a natural number $N \in \mathbb{N}$ an $N$-torsion $[z] \in E$ is an element with $Nz = 0$ in $E$, or equivalently $Nz \in \Lambda$. The subgroup of $E$ of $N$-torsions is

$$E[N] := \{ z \in E | Nz = 0 \} \simeq \frac{\mathbb{Z}_N}{\Lambda}$$

\[ \simeq \left\{ \frac{a\omega_1 + b\omega_2}{N} \middle| a, b \in \mathbb{Z} \right\} \simeq \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}} \]

The following definition of Weil pairing is taken from [Silverman II], page 89.

**Definition 9.2.1** Let $E$ be an elliptic curve. The Weil pairing is

$$e_N : E[N] \times E[N] \to \mu_N$$

\[ e_N \left( \frac{a\omega_1 + b\omega_2}{N}, \frac{c\omega_1 + d\omega_2}{N} \right) = e^{2\pi i \text{Re} \frac{ad - bc}{N}} \]

Here

$$\mu_N := \{ e^{\frac{2\pi i k}{N}} \mid k \in \mathbb{Z} \}. $$

**Exercise 57** Prove that the above definition is well-defined.

**Theorem 9.2.1** Let

$$Y_0(N) := \Gamma_0(N) \setminus \mathbb{H}, \ Y_1(N) := \Gamma_1(N) \setminus \mathbb{H}, \ Y(N) := \Gamma(N) \setminus \mathbb{H}. $$

1. The set $Y_0(N)$ is the moduli space of pairs $(E, C)$, where $E$ is a complex elliptic curve and $C$ is a cyclic subgroup of $E$ of order $N$.
2. The set $Y_1(N)$ is the moduli space of pairs $(E, p)$, where $E$ is a complex elliptic curve and $p$ is a point of $E$ of order $N$. 

9.4 Modular forms for congruence groups

3. The set \( Y(N) \) is the moduli space of pairs \((E, (p, q))\), where \( E \) is a complex elliptic curve and \((p, q)\) is a pair of points of \( E \) that generates the \( N \)-torsion subgroup of \( E \) with Weil pairing \( e_N(p, q) = e^{\frac{2\pi i}{N}} \).

*Proof.* We only prove item 2. The others are left to the reader.

**Exercise 58** Prove items 1 and 3 above.

9.3 Moduli spaces of elliptic curves

We consider the following moduli spaces, which we call them period domains. The difference between these moduli spaces and those in theorem (9.2.1) is the presence of the differential form \( \omega \) together with \( E \). Recall that by integration the pair \((E, \omega)\) is identified with a lattice \( \Lambda \subset \mathbb{C} \).

\[
\mathcal{P} := \text{moduli of elliptic curves } (E, \omega),
\]

\[
\mathcal{P}_1(N) := \text{moduli of } (E, \omega, z), \ z \in E[N]
\]

\[
\mathcal{P}(N) := \text{moduli of } (E, \omega, \{z_1, z_2\}), \ z_1, z_2 \in E[N], \ e_N(z_1, z_2) = \zeta_N
\]

\[
\mathcal{P}_0(N) := \text{moduli of } (E, \omega, C), \ C \subseteq E[N] \text{ cyclic group of order } N.
\]

Let \( f \) be an elliptic function of weigh \( k \) with poles at 0. For instance, we use \( \wp, \wp' \) which are of weight 2 and 3, respectively. We know the following functions on period domains

\[
f_{1,N} : \mathcal{P}_1(N) \to \mathbb{C}, \quad f_{1,N}(E, z) = f(\Lambda, z)
\]

\[
f_N : \mathcal{P}(N) \to \mathbb{C}, \quad f_N(E, z_1, z_2) = f(\Lambda, z_i), \ i = 1, 2
\]

\[
f_{0,N} : \mathcal{P}_0(N) \to \mathbb{C}, \quad f_{0,N}(E, C) = f(\Lambda, z) = \sum_{z \in C} f(\Lambda, z)
\]

Any function \( g \) as above has the following functional equation:

\[
g(E, a\omega, *) = a^{-k} g(E, \omega, *), \ \forall a \in \mathbb{C}^*.
\]

where \( k \) is the weight of the elliptic function \( f \).

9.4 Modular forms for congruence groups

We consider the following maps
\[ i : \mathbb{H} \to \mathcal{P}_1(N) \quad \tau \mapsto (E, \omega, \frac{1}{N}) \]
\[ i : \mathbb{H} \to \mathcal{P}(N) \quad \tau \mapsto \left(E, \omega, \left(\frac{\tau}{N}, \frac{1}{N}\right)\right) \]
\[ i : \mathbb{H} \to \mathcal{P}_0(N) \quad \tau \mapsto \left(E, \omega, \left\{\frac{1}{N}, \frac{2}{N}, \ldots, \frac{N-1}{N}\right\}\right) \]
here \( E = \mathbb{C}/\mathbb{Z} \tau + \mathbb{Z} \) and \( \omega = dz \)

**Proposition 9.4.1** Let \( f \) be an elliptic function of weight \( k \) with poles at \( 0 \). Then the pull-back of \( f \) by \( i \) is a holomorphic modular form of weight \( k \) for \( \Gamma_1(N) \), \( \Gamma(N) \), and \( \Gamma_0(N) \) respectively.

**Proof.** We only prove the \( \mathcal{P}_1(N) \) case

\[
f_{1,N} \left(\frac{a\tau + b}{c\tau + d}\right) = f \left(\frac{\mathbb{Z}(a\tau + b) + \mathbb{Z}, \frac{1}{N}}{c\tau + d}\right)
\]

\[
= (c\tau + d)^+ f(\mathbb{Z}\tau + \mathbb{Z}, \frac{1}{N})
\]

For all \( \left(\frac{a\ b\ c\ d}{1\ 0}\right) \in \Gamma_1(N) \). Now we have to show the growth condition. For this it is enough to assume that \( f = \wp \) or \( \wp' \). In these cases the affirmation follows from

\[
\lim_{\text{Im}(\tau) \to \infty} \wp(\mathbb{Z}\tau + \mathbb{Z}, z) = \sum_{m \in \mathbb{Z}} \frac{1}{(z-m)^2} - \frac{1}{m^2}
\]

\[
\lim_{\text{Im}(\tau) \to \infty} \wp'(\mathbb{Z}\tau + \mathbb{Z}, z) = -2 \sum_{m \in \mathbb{Z}} \frac{1}{(z-m)^3}
\]

\[ \square \]

**Exercise 59** Show that

\[
\#[\text{SL}(2,\mathbb{Z}) : \Gamma_1(N)] = \deg(\mathcal{P}_1(N) \to \mathcal{P}) = n^2 \prod \left(1 - \frac{1}{p^2}\right)
\]

\[
\#[\text{SL}(2,\mathbb{Z}) : \Gamma(N)] = \deg(\mathcal{P}(N) \to \mathcal{P}) = n^3 \prod \left(1 - \frac{1}{p^3}\right)
\]

\[
\#[\text{SL}(2,\mathbb{Z}) : \Gamma_0(N)] = \deg(\mathcal{P}_0(N) \to \mathcal{P}) = n \prod \left(1 - \frac{1}{p}\right)
\]

### 9.5 q-expansion

Let \( f \) be a modular form for a congruence group \( \Gamma \) of level \( N \). It follows that for all \( A \in \text{SL}(2,\mathbb{Z}) \), \( f|_A \) has a q-expansion. Let
9.5 \( q \)-expansion

\[ q_N := e^{\frac{2\pi i}{N}} \]

We have

\[ T = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad T^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N) \]

and so

\[ (f|_k A)T^N = f|_k (AT^N A^{-1}) A = f|_k A \]

This implies that

\[ f|_k A = \sum_{n=0}^{\infty} a_n q^n, \quad a_n \in \mathbb{C}. \]

**Proposition 9.5.1** If \( f \) is a modular form of weight \( k \) for \( \text{SL}(2, \mathbb{Z}) \) then \( g(\tau) := f(N\tau) \) is a modular form of weight \( k \) for \( \Gamma_0(N) \).

**Proof.** First note that \( N^{k-1} g = f|_k \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \) and so \( g(\tau) \) is a priori a modular form for

\[ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \text{SL}(2, \mathbb{Z}) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}. \]

For \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \) we have

\[ \begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & N^{-1}b \\ Nc & d \end{pmatrix} \]

which means that \( g \) is modular for \( \Gamma_0(N) \).

**Exercise 60** Compute the \( q \)-expansions of \( \wp_{1,N}, \wp_{N}, \wp_{0,N} \).

We can construct modular functions for congruence groups by division for instance:

\[ \varphi(\tau) := \frac{\Delta(N\tau)}{\Delta(\tau)} \]

is a modular function for the group \( \Gamma_0(N) \). This follows from the functional equation of \( \Delta(\tau) \) is follows that \( \varphi \) is holomorphic in \( \mathbb{H} \). It is also holomorphic at \( i\infty \):

\[ \varphi(\tau) = \frac{q^N \prod_{n=1}^{\infty} (1 - q^{nN})^{24}}{q \prod_{n=1}^{\infty} (1 - q)} = q^{N-1} \left( 1 + \sum_{n=1}^{\infty} b_n q^n \right) \]

and actually it has a zero of order \( N - 1 \) at \( q = 0 \). There are no non-constant holomorphic functions on a compact Riemann surface, and so, \( \varphi \) as a function on \( \mathbb{H} \) is necessarily meromorphic. Since in \( \Gamma_0(N) \setminus \mathbb{H} \cup \{i\infty\} \) it has only one zero which is
of order $N - 1$ doing q-expansions in other cusps we must have poles. For this we use

$$\sum_{* \in \Gamma_0(N) \setminus \mathbb{Q}} \text{ord}_*(f) = 0$$

Note that the Fourier coefficients $b_n$ of $\varphi$ are integers. For more information on $\varphi$ see Apostol’s book [Apostol], section 4.7

### 9.6 Transcendental degree of modular forms

Let $\Gamma \subseteq SL(2, \mathbb{Z})$ be a subgroup of finite index $a$. Let also $f \in M_k(\Gamma)$. We define

$$\sum_{i=0}^{a} g_{a-i} \cdot X^i = \prod_{A \in \Gamma \setminus SL(2, \mathbb{Z})} (X - (f|_kA),\ g_0 := 1 \quad (9.2)$$

**Proposition 9.6.1** We have $g_i \in M_k(\Gamma, SL(2, \mathbb{Z}))$.

**Proof.** Let $P(X)$ be the right hand side of (9.2). Then for $B \in SL(2, \mathbb{Z})$ we have

$$P(X)|_kB = \prod_{A \in \Gamma \setminus SL(2, \mathbb{Z})} (X - (f|_kA)|_kB) = P(X)$$

Therefore, the coefficients of $P(X)$ has the correct functional equation. The finite growth of $g_i$’s follow from the finite growth of $f|_kA$’s for all $A \in \Gamma \setminus SL(2, \mathbb{Z})$. \(\square\)

Conversely, let us be given $g_i \in M_k(\Gamma, SL(2, \mathbb{Z}))$, $i = 1, 2, .., a$, and define

$$P(X) = \sum_{i=0}^{a} g_{a-i} \cdot X^i$$

The resultant of $P(X)$ is a homogeneous polynomial of degree $2 \cdot k \cdot a$ in

$$Q[g_1, g_2, \ldots, g_a], \ weight(g_i) = ki$$

This is a weight $2ka$ modular form for $SL(2, \mathbb{Z})$. Assume that this resultant has no zeros. Since $\mathbb{H}$ is simply connected, we can find holomorphic functions $f_1, f_2, \ldots, f_a : \mathbb{H} \to \mathbb{C}$ such that

$$P(X) = (X - f_1)(X - f_2) \cdots (X - f_a)$$

We have the representation

$$\chi : SL(2, \mathbb{Z}) \to GL(a, \mathbb{Z})$$

whose image is isomorphic to the permutation group in $a$ elements and such that
\[
\begin{pmatrix}
  f_1 | kA \\
  f_2 | kA \\
  \vdots \\
  f_a | A
\end{pmatrix}
= \chi(A) \begin{pmatrix}
  f_1 \\
  f_2 \\
  \vdots \\
  f_a
\end{pmatrix}, \quad \forall A \in \text{SL}(2, \mathbb{Z}).
\] (9.3)

Here \( \chi(A) \) is just a permutation matrix in \( 1, 2, \ldots, a \). Let

\[
\Gamma_i := \{ A \in \text{SL}(2, \mathbb{Z}) | \chi(A)e_i = e_i \}
\]

where \( e_i = [0, 0, \ldots, 1, \underbrace{0, \ldots, 0}_{i-th \text{ place}}]^{tr} \).

**Proposition 9.6.2** We have \( f_j \in M_k(\Gamma_i) \).

**Proof.** This is a direct consequence of (9.3) and the definition of \( \Gamma_i \). \( \square \)

**Exercise 61** Show that \( P(X) \) is irreducible over \( M_k(\text{SL}(2, \mathbb{Z})) \)[\( X \] if and only if an orbit of \( \chi \) in \( \{1, 2, \ldots, a\} \) is the whole set. It follows that if \( P(X) \) is irreducible over \( M_k(\text{SL}(2, \mathbb{Z})) \)[\( X \]. Then

\[
\{f_1, f_2, \ldots, f_a\} = \{f_i | kA, \quad A \in \Gamma \setminus \text{SL}(2, \mathbb{Z})\}
\]

\[
\Gamma_i := A^{-1} \cdot \Gamma_i A \quad A \in \Gamma \setminus \text{SL}(2, \mathbb{Z})
\]

The following question is natural to ask: under which conditions on \( g_i \)'s, \( \Gamma_i \) is a congruence group? We have proved:

**Theorem 9.6.1** The ring of modular forms for congruence groups is of transcendental degree 2. More precisely any modular form for a congruence group is in the algebraic closure of \( \mathbb{C}(E_4, E_6) \).
Chapter 10
Elliptic curves as Diophantine equations

10.1 Finite fields

A finite field, as its name indicates, is a field with finite cardinality. By definition of a field and finiteness property, the characteristic of a finite field is a prime number \( p > 1 \). Finite fields are completely classified as follows:

1. The order of a finite field of characteristic \( p \) is \( p^n \) for some \( n \in \mathbb{N} \).
2. There is a unique (up to isomorphism of fields) finite field with \( p^n \), \( n \in \mathbb{N} \) elements.
3. For a prime number the finite field with cardinality \( p \) is simply the quotient
   \[
   \mathbb{F}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}.
   \]
4. For \( q = p^n \), \( n \in \mathbb{N} \) the finite field with cardinality \( p^n \) is denoted by \( \mathbb{F}_q \). It is the splitting field of the polynomial \( x^q - x \) over \( \mathbb{F}_p \).
5. Every finite integral domain is a field and in particular
6. Let \( f(T) \) be a monic irreducible polynomial of degree \( n \) in \( \mathbb{F}_p[T] \). Then the quotient \( \mathbb{F}_q[T]/(f) \) is a finite field with \( p^n \) elements.
7. Let \( f(x,y) \in \mathbb{F}_p[x,y] \) be a polynomial and \( I \) be a non zero prime ideal of \( R := \mathbb{F}_p[x,y]/(f) \). Then the quotient \( R/I \) is a finite field.

For more on finite fields the reader is referred to [Jac85].

10.2 Zeta functions of elliptic curves over finite fields

Let \( V \) be an affine or projective variety defined over \( \mathbb{F}_q \). The zeta function of \( V \) is defined to be the formal power series in \( T \):
Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Then

$$Z(E, T) = \frac{1 + 2a_E T + pT^2}{(1 - T)(1 - pT)}.$$  \hfill (10.1)

where $a_E$ is an integer depending only on $E$. Moreover, the Riemann hypothesis holds for $E$, i.e. the only zeros of

$$\zeta(C, s) := Z(E, q^{-s})$$

are in the line $\Re(s) = \frac{1}{2}$.

Let

$$1 - 2a_E T + qT^2 = (1 - \alpha T)(1 - \beta T)$$

and so

$$\alpha + \beta = 2a_E, \quad \alpha\beta = q \quad (10.2)$$

Note that $\alpha$ and $\beta$ are algebraic integers:

$$\alpha, \beta = a_E \pm \sqrt{a_E^2 - q}.$$  

We take the logarithmic derivative of both sides of (10.1) and one easily finds the equalities

$$\#E(F_{p^r}) = p^r + 1 - \alpha^r - \beta^r, \quad r = 1, 2, 3, \ldots$$

For $r = 1$ we obtain

$$\#E(F_p) = p + 1 - 2a_E$$

We conclude that for elliptic curves over a finite field $\mathbb{F}_q$ the number of $\mathbb{F}_q$-rational points determines the number of $\mathbb{F}_{q^r}$-rational points.

Concerning the Riemann hypothesis, we note that it is equivalent to the inequality:

$$|\#E(F_p) - p - 1| < 2\sqrt{p}. \quad (10.3)$$

The Riemann hypothesis holds if and only if $|\alpha| = |\beta| = p^{\frac{1}{2}}$. If these equalities happen then

$$|\#E(F_p) - p - 1| = |2a_E| = |\alpha + \beta| < 2\sqrt{p}.$$  

The equality cannot occur because $p$ is prime. Conversely, if (10.3) happens then $a_E^2 - p < 0$ and so the roots of the polynomial $1 - 2a_E T + qT^2$ are complex conjugate, $\beta = \bar{\alpha}$ and so $|\alpha| = |\beta| = p^{\frac{1}{2}}$.

The general result as in (10.1) was conjectured by André Weil [Wei49] and was proved by P. Deligne (see for instance [Kat76] for an exposition of Deligne results).
10.3 Nagell-Lutz Theorem

In this section we state Nagell-Lutz theorem which gives a finite set of of possibilities for a torsion point of an elliptic curve.

**Theorem 10.3.1** (Nagell-Lutz Theorem) Let $E$ be an elliptic curve with the Weierstrass equation:

$$y^2 = x^3 + t_2x + t_3, \quad t_2, t_3 \in \mathbb{Z}, \Delta := 4t_3^2 + 27t_2^3 \neq 0.$$  

Then for all non-zero torsion points $P = (a, b) \in E(\mathbb{Q})$ we have:

1. The coordinates of $P$ are in $\mathbb{Z}$, i.e. $a, b \in \mathbb{Z}$.
2. If $P$ is of order greater than 2, then $b^2$ divides $\Delta$.
3. If $P$ is of order 2 then $b = 0$ and $a^3 + t_2a + t_3 = 0$.

A proof can be found in [Sil92], p. 221 or in [ST92] p.56.

**Exercise 62** [Mil96], Exercise 8.11. For four of the following elliptic curves compute the torsion subgroup.

$$y^2 = x^3 + 2, \cdots$$

See the reference above for the list of elliptic curves.

10.4 Mazur theorem

**Theorem 10.4.1** (Mazur, [Maz77, Maz78]) Let $E$ be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of the following fifteen groups:

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10, \quad \text{or } N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4$$

Note that the above theorem implies that for an elliptic curve over $\mathbb{Q}$ we have always:

$$\#(E(\mathbb{Q})_{\text{tors}}) \leq 16.$$  

It is natural to conjecture that: If $E$ is an elliptic curve over a number field $k$, the order of the torsion subgroup of $E(k)$ is bounded by a constant which depends only on the degree of $k$ over $\mathbb{Q}$. This is known uniform boundedness conjecture (UBC). It is proved by S. Kamienny in [Kam92] for all quadratic fields and by L. Merel in [Mer96] for all number fields.

For the proof of all the statements above one needs the notion of modular curves $X_0(N)$ and modular forms which will be introduced in the forthcoming chapters.
10.5 One dimensional algebraic groups

We follow [Mil96] p. 23. When elliptic curves degenerate we find the following algebraic groups:

1. The additive group $\mathbb{G}_a := (\mathbb{A}^1(k), +)$.
2. The multiplicative group $\mathbb{G}_m := (\mathbb{A}(k)^*, \cdot)$.
3. Twisted multiplicative group $\mathbb{G}_m^a$.

**Exercise 63**

\[ \mathbb{G}_m[a] \cong \mathbb{G}_m[ac^2], \quad a, c \in k - 0, \]

**Exercise 64**

\[ \mathbb{G}_m[a](\mathbb{F}_q) = q + 1. \]

By Bezout theorem a cubic curve $E$ in $\mathbb{P}^2$ has a unique singular point (if there are two singularities then the line connecting that points meets the curve in 4 points counted with multiplicities). The singular point is defined over $k$ because it is fixed under the action of the Galois group $Gal(\overline{k}/k)$. Let $S$ be the singular point of $E$ and

\[ E^{ns}(k) := E(k) \setminus \{S\}. \]

The same definition of group law for elliptic curves applies for $E^{ns}$ and it turns out that $E^{ns}$ as a group and:

**Exercise 65** If the elliptic curve $E$ is given by the Weierstrass form

\[ y^2 = x^3 + t_4x + t_6, \quad t_2, t_3 \in k, \Delta = 2(4t_4^3 + 27t_6^2) = 0. \]

then $E^{ns}$ is isomorphic to the three one dimensional group described above:

\[ E^{ns}(k) \cong \mathbb{G}_m(k) \text{ or } \mathbb{G}_m[c](k), \text{ or } \mathbb{G}_a(k) \]

mentioned in the lectures. Does we need $\text{char}(k) \neq 2, 3$?

**Exercise 66** For $\text{char}(k) = 3$ (resp. $\text{char}(k) = 2$) we have to consider the case (4.6) (resp. (4.4)). Discuss the reduction modulo 2 and 3 in such cases.

10.6 Reduction of elliptic curves

We take an elliptic curve in the Weierstrass form

\[ y^2 = x^3 + t_4x + t_6, \quad t_2, t_3 \in \mathbb{Q}, \Delta := 2(4t_4^3 + 27t_6^2) \neq 0. \]

and by change of coordinates $(x, y) \mapsto (c^2x, c^3y), \ c \in \mathbb{Q}$ we assume that $|\Delta|$ is minimal. For $p$ prime different from 2 and 3 we have the curve $E/\mathbb{F}_p$ and the reduction map
10.7 Zeta functions of curves over \( \mathbb{Q} \)

We follow [Mil96] p. 102. The non-complete zeta function of a smooth curve \( E : f(x,y) = 0, \ f \in \mathbb{Z}[x,y] \) is defined to be

\[
\zeta_S(E,s) = \prod_{p \notin S} \zeta(E/F_p,s).
\]

where \( S \) is a finite number of prime numbers such that \( E/F_p \) is singular.

**Exercise 69** Can you justify the definition of the zeta function of a variety over \( \mathbb{Q} \) by interpreting it as a Euler product, the one similar to (8.11). In the case of elliptic curves it is natural to define

\[
L_S(E,s) := \prod_{p \notin S} \frac{1}{1 + (\#(E(F_p)) - p - 1)p^s + p^{s-2}}
\]

and so we have

\[
\zeta_S(E,s) = \frac{L_S(E,s)\zeta_S(s-1)}{L_S(E,s)}
\]

**Proposition 10.7.1** The product \( \zeta_S(E,s) \) and hence \( L_S(E,s) \) converges for \( \Re(s) > \frac{3}{2} \)

**Proof.** It is direct consequence of the Riemann hypothesis for elliptic curves over finite fields and the convergence of the Riemann zeta function (see [Mil96] p.102).
We we want to define the complete $L$ function by adding bad prime numbers $p \in S$. We define

$$L_p(T) = \begin{cases} 
1 + \left( \#(E(F_p)) - p - 1 \right) T + pT^2 & p \text{ good} \\
1 - T & \text{modulo } p \text{ we have split multiplicative reduction} \\
1 + T & \text{modulo } p \text{ we have non-split multiplicative reduction} \\
1 & \text{modulo } p \text{ we have additive reduction}
\end{cases}$$

We have defined this in such a way that

$$L_p(p-1) = \frac{\#E_{ns}(F_p)}{p}$$

Now we define the $L$-function of an elliptic curve $E$ over $\mathbb{Q}$:

$$L(E, s) = \prod_p \frac{1}{1 - L_p(p^{-s})}.$$

### 10.8 Hasse-Weil conjecture

The conductor of an elliptic curve over $\mathbb{Q}$ is defined to be

$$N_{E/\mathbb{Q}} = \prod_{p \text{ bad}} p^{f_p}$$

where $f_p = 1$ if $E$ has multiplicative reduction at $p$, $f_p = 2$ if $p \nmid 2, 3$ and $E$ has additive reduction at $p$. For the case in which we have additive reduction modulo $p = 2, 3$ we have $f_p \geq 2$, $f_p \in \mathbb{N}$ and $f_p$ depends on wild ramification in the action of the inertia group at of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module of $E$.

**Exercise 70** Discuss the case $p = 2, 3$ in the above definition. [Mil96] is also talking about a formula of Ogg $f_p = \text{ord}_p \Delta + 1 - m_p$ using Néron models. Can you obtain some information on this.

Define

$$\Lambda(E, s) := N_{E/\mathbb{Q}}^{\frac{1}{2}}(2\pi)^{-s} \Gamma(s)L(E, s)$$

**Theorem 10.8.1** (Hasse-Weil conjecture for elliptic curves) The function $\Lambda(E, s)$ can be analytically continued to a meromorphic function on the whole $\mathbb{C}$ and it satisfies the functional equation

$$\Lambda(E, s) = \pm \Lambda(E, 2 - s).$$

This theorem was first proved for CM elliptic curves by Deuring 1951/1952. It is proved in its generality by the works of Eichler and Shimura, Wiles, Taylor, Diamond and others.
10.9 Birch Swinnerton-Dyer conjecture

For the functional equation of $L$ the value $s = 1$ is in the middle, i.e. it is the fixed point of $s \mapsto 2 - s$.

Conjecture 10.9.1 (BSD conjecture) For an elliptic curve $E$ over $\mathbb{Q}$, the function $L(E, s)$ is holomorphic at $s = 1$ and its order of vanishing at $s = 1$ is the rank of the elliptic curve $E$.

A weak form of this conjecture is not also proved:

Conjecture 10.9.2 (weak BSD conjecture) $L(E, 1) = 0$ if and only if $E$ has infinitely many rational points.

For papers on BSD conjecture see [CW77, BSD63, BSD65, Tun83, Lan78b, Ser89, Mor69].

10.10 Congruent numbers

A natural number $n$ is said to be congruent if it is the area of a right triangle whose sides have rational length. In other words we are looking for the Diophantine equation:

$$ C_n : x^2 + y^2 = z^2, \quad n = \frac{1}{2}xy $$

in $\mathbb{Q}$, where $x, y$ and $z$ are the sides of the triangle. Consider the affine curve $C_n/\mathbb{Q}$ in $\mathbb{A}^3$ defined by the above equations. It intersects the projective space at infinity in 4 points:

$$ [x; y; z; w] = [0; \pm 1; 1; 0], \quad [\pm 1; 0; 1; 0]. $$

Let

$$ C : y^2 = x^4 - n^2, \quad E_n : y^2 = x^3 - n^2x. $$

We have morphisms

$$ C_n \to C, \quad (x, y, z) \mapsto \left( \frac{z}{2}, \frac{x^2 - y^2}{4} \right) $$

and

$$ C \to E_n, \quad (x, y) \mapsto (x^2, xy) $$

defined over $\mathbb{Q}$.

Proposition 10.10.1 A necessary and sufficient condition for the point $(x, y) \in E_n(\mathbb{Q})$ to be in the image of $C_n(\mathbb{Q}) \to E_n(\mathbb{Q})$ is that

1. $x$ to be a square and that
2. its denominator be divisible by two
3. and its numerator has no common factor with $n$.

The proof is simple and is left to the reader (see [Kob93]).
**Exercise 71** Let $\overline{C_n}$ be the projectivization of $C_n$ in $\mathbb{P}^3$. Is $\overline{C_n}$ smooth? If yes determine its genus.

**Exercise 72** Ex. 1,2,3,4 of Koblitz, page 5.

We want to analyze the torsion points of $E_n$:

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

By definition of the group structure of $E_n$ we know that $O, (0, 0), (0, \pm n)$

are 2-torsions of $E_n$. Following the lines of [Kob93] p. 44 Proposition 4, we want to prove:

**Proposition 10.10.2** We have

$$E_n(\mathbb{Q})_{\text{tors}} = \{O, (0, 0), (0, \pm n)\}$$

and so $\#E_n(\mathbb{Q})_{\text{tors}} = 4$.

**Proof.** Let us first give the strategy of the proof. Let $E/\mathbb{Q}$ be an elliptic curve in the Weierstrass form and let $p > 2$ be a prime number which does not divide the discriminant of $E$. By a linear change of variable $(x, y) \mapsto (a^2 x, a^3 y)$ we can assume that the ingredient coefficients of $E$ are in $\mathbb{Z}$. Let $\overline{E}/\mathbb{F}_p$ be the elliptic curve obtained from $E$ by considering the coefficients of $E$ modulo $p$. The main ingredient of the proof is the reduction map

$$E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p),$$

which is a group homomorphism. Note that by our assumption on $p$, $\overline{E}/\mathbb{F}_p$ is not singular. This is an injection of $E(\mathbb{Q})_{\text{tors}}$ inside $E(\mathbb{F}_p)$ for all but finitely many $p$ and so for such primes $m := \#E(\mathbb{Q})_{\text{tors}}$ divides $\#E(\mathbb{F}_p)$. In fact, we have not yet proved that $E(\mathbb{Q})_{\text{tors}}$ is finite (a corollary of Mordell-Weil theorem). Therefore, we take a finite subgroup $G$ of $E(\mathbb{Q})_{\text{tors}}$ and prove that the reduction map restricted to $G$ is an injection and so $m := \#G$ divides $\#E(\mathbb{F}_p)$. From another side, we prove that for $E = E_n$:

$$\#E_n(\mathbb{F}_p) = p + 1, \forall p \text{ prime } p \equiv -1 \mod 4 \quad (10.4)$$

Therefore, for all but finitely many primes $p \equiv -1 \mod 4$ we have $p \equiv -1 \mod m$. This implies that $m = 4$. Therefore, every finite subgroup of $E(\mathbb{Q})_{\text{tors}}$ is of order 4. Since all the elements of $E(\mathbb{Q})_{\text{tors}}$ are torsion, we conclude that $\#E_n(\mathbb{Q})_{\text{tors}} = 4$.

Now let us prove that the reduction map induces an injection in a finite subgroup $G$ of $E(\mathbb{Q})_{\text{tors}}$. Two points $P = [x; y; z], Q = [x'; y'; z'] \in E(\mathbb{Q})$ are the same after reduction if and only if

$$xy' - x'y, xz' - x'z, yz' - y'z \quad (10.5)$$

are zero modulo $p$. For all pairs $P, Q$ in $G$, the number of numbers $\text{[10.5]}$ is finite and so there are finitely many primes dividing at least one of them. For all other primes
10.10 Congruent numbers

Let \( p \), we have the injection of \( G \) in \( E(\mathbb{F}_p) \) by the reduction map. The proof of \( \text{(10.4)} \) is done in the next proposition.

**Proposition 10.10.3** Let \( q = p^f, \ p \nmid 2n \). Suppose that \( q \equiv -1 \mod 4 \). Then there are \( q+1 \) \( \mathbb{F}_q \) points on the elliptic curve \( E_n : y^2 = x^3 - n^2x \).

**Proof.** Consider the map

\[
f : \mathbb{F}_q \to \mathbb{F}_q, \ f(x) = x^3 - n^2x
\]

\( f \) is an odd function, i.e. \( f(-x) = -f(x) \), and \(-1\) is not in its image (this follows from the hypothesis on \( p \)). It follows that the index of the multiplicative group \( \mathbb{F}_q^2 = \{0\} \) in \( \mathbb{F}_q - \{0\} \) is two and so for all \( x \in \mathbb{F}_q - \{0\} \) exactly one of \( x \) or \(-x\) is square and so for all \( x \in \mathbb{F}_q - \{0,n,-n\} \) exactly one of \( f(x) \) or \( f(-x) \) is square. Each such a pair \((x,y), y = f(x) \) gives us two points \((x,y), (x,-y) \in E_n(\mathbb{F}_q) \) and so in total we have \( 3 + 2\frac{q-1}{2} \) points in \( E_n(\mathbb{F}_q) \).

**Proposition 10.10.4** The natural number \( n \) is congruent if and only if \( E_n(\mathbb{Q}) \) has non-zero rank.

**Proof.** If \( n \) is a congruent number then by Proposition 10.10.1, \( E_n \) has \( \mathbb{Q} \)-rational point with \( x \)-coordinate in \( (\mathbb{Q}^+) \times \times C_n(\mathbb{Q}) \). The \( x \)-coordinates of \( 2 \)-torsion points in the affine chart \( x, y \) are \( 0, \pm n \). The fact that \( n \) is square free and Proposition 10.10.2 implies that such a rational point is of infinite order.

Conversely, suppose that \( P \) is a rational point of infinite order in \( E_n \). Then by Exercise 73, the

**Exercise 73 (Kob93), p. 35, Ex. 2c)** If \( P \) is a point not of order 2 in \( E_n(\mathbb{Q}) \), then the \( x \)-coordinate of \( 2P \) is a square of rational number having an even denominator. By Proposition 10.10.1 \( 2P \) comes from a point in \( C_n(\mathbb{Q}) \) and hence \( n \) is a congruent number.

**Exercise 74 (Kob93), p. 49-50** Ex. 4, 5, 6, 7, 9.

Let us now state the main result in \( \text{(10.2)} \) for the elliptic curve \( E_n \) related to the congruent numbers. The Legendre symbol is defined for integers \( a \) and positive odd primes \( p \) by

\[
\left( \frac{a}{p} \right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ 1 & \text{for some } x \in \mathbb{Z}, \ a \equiv x^2 \mod p \\ -1 & \text{otherwise} \end{cases}
\]

**Proposition 10.10.5** In the zeta function of \( E_n : y^2 = x^3 - n^2x \) defined over \( \mathbb{F}_p, p \) a prime \( p \nmid 2n \), we have:

\[
\alpha = \begin{cases} i\sqrt{p} & \text{if } p \equiv 3 \mod 4 \text{ in this case } a_{E_n} = 0 \\ 2k + \left( \frac{a}{p} \right) + 2ki & \text{if } p \equiv 1 \mod 4 \text{ in this case } a_{E_n} = 2k + \left( \frac{a}{p} \right) \end{cases}
\]

In the second case \( k \) is determined by the fact that \( \alpha \bar{\alpha} = p \).
**Exercise 75** ([Mil96], Ex. 19.12) Let \( E \) be the elliptic curve

\[
E : y^2 = x^3 - 4x^2 + 16
\]

Consider also the formal power series given by

\[
F(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2 = q - 2q^2 - q^3 + 2q^4 + \cdots
\]

1. Compute \( N_p = \#E(\mathbb{F}_p) \) for all primes \( 3 \leq p \leq 13 \).
2. Calculate the coefficient of \( M_n \) of \( q^n \) in \( F(q) \) for \( n \leq 13 \).
3. Compute the sum \( M_p + N_p \) for \( p \) prime \( p \leq 13 \).
4. Formulate a conjecture on the sum \( M_p + n_p \). Can you prove it?

The bad prime numbers for the elliptic curve \( E_n : y^2 = x^3 - nx \) are those which divide \( 2n \). For \( p | 2n \), \( p \neq 2 \) or \( p = 2 \), \( 2 | n \) we have an additive reduction. For \( p = 2 \) and \( p \nmid n \) we have apparently a multiplicative reduction: \( y^2 = x^3 + x \). The singular point in this case is \( S = (1,0) \) and \( E_n^s(\mathbb{F}_2) = \{ O, (0,0) \} \) which is isomorphic to \( (\mathbb{A}(\mathbb{F}_2), +) \) and so it is additive.

The conductor of \( E_n \) is:

\[
N_{E_n/Q} = \begin{cases} 2^4n^2 & \text{if } n \text{ is even} \\ 2^5n^2 & \text{if } n \text{ is odd} \end{cases}
\]

In Theorem [10.8.1] the root number \( \pm \) is determined in the following way:

\[
\begin{cases} +1 & \text{if } n \equiv 1, 2, 3 \pmod{8} \\ -1 & \text{if } n \equiv 5, 6, 7 \pmod{8} \end{cases}
\]

Reformulating Proposition [10.10.5] and using Exercise [55] we have:

\[
(1 - T)(1 - pT)Z(E_n/\mathbb{F}_p, T) = \prod_{p|n} (1 - (\alpha_p T)^{\deg(p)})
\]

where

\[
\alpha_p = \begin{cases} i\sqrt{p} & \text{if } p = \langle p \rangle \\ a + ib & \text{if } p \text{ splits, where } a + ib \text{ is the unique generator of } p \text{ which is congruent to } (\frac{2}{p}) \text{ mod } 2 + 2i. \\ 0 & \text{if } p \nmid 2n \end{cases}
\]

The \( L \) function of \( E_n \) is

\[
L(E_n, s) = \prod_{p \in \mathbb{Z}[i] \text{ prime}} (1 - (\alpha_p)^{\deg(p)}(N[p])^{-s})^{-1}
\]

Now \( \mathbb{Z}[i] \) is a Dedekind domain and so we can define a unique map \( \chi \) from the ideals of \( \mathbb{Z}[i] \) to \( \mathbb{C} \) such that \( \chi_a(p) = \alpha_p^{\deg(p)} \). Therefore
\[
L(E_n, s) = \prod_{p \in \mathbb{Z}[l] \text{ prime}} (1 - \chi(p)(Np)^{-s})^{-1} = \sum_{a \in \mathbb{Z}[l]} \chi_n(a)(Na)^{-s}
\]

where the sum is taken over all non-zero ideals.

10.11 \( p \)-adic numbers

By definition a \( p \)-adic integer is an element in the inverse limit of
\[
\cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}
\]
One can show that a \( p \)-adic integer is identified with a formal series
\[
a_1p + a_2p^2 + a_3p^3 + \cdots, \ a_i \in \{0, 1, 2, \ldots, p-1\}.
\]
The set of \( p \)-adic integers is denoted by \( \mathbb{Z}_p \):
\[
\mathbb{Z}_p := \lim_{\longrightarrow \ n} \mathbb{Z}/p^n\mathbb{Z}.
\]
\( \mathbb{Z}_p \) is a ring without zero divisor, i.e. if \( ab = 0, a, b \in \mathbb{Z}_p \) then either \( a = 0 \) or \( b = 0 \). The field \( \mathbb{Q}_p \) of \( p \)-adic numbers is the quotient field of \( \mathbb{Z}_p \). The ring \( \mathbb{Z} \) of integers is a subring of \( \mathbb{Z}_p \) in a natural way and so \( \mathbb{Q}_p \) is a field extension of \( \mathbb{Q} \), \( \mathbb{Q} \subset \mathbb{Q}_p \).

Exercise 76 Show that the Diophantine equation \( x^3 + y^3 - 3 = 0 \) has not a solution in \( \mathbb{Q}_3 \) and hence it has not a solution in \( \mathbb{Q} \).

There is another way to define \( p \)-adic numbers. Any non-zero rational number \( a \) can be expressed in the form \( a = p^n \frac{m}{n} \) with \( m, n \in \mathbb{Z} \) and not divisible by \( p \). We define
\[
\text{ord}_p(a) := r, \ |a|_p := \frac{1}{p^r}, \ |0|_p := 0
\]
We have
1. \( |a|_p = 0 \) if and only if \( a = 0 \)
2. \( |ab|_p = |a|_p|b|_p, \ a, b \in \mathbb{Q} \)
3. \( |a + b|_p \leq \max\{|a|_p, |b|_p\} \) and so \( \leq |a|_p + |b|_p \)
Therefore,
\[
d_p(a, b) := |a - b|_p
\]
is a metric on \( \mathbb{Q} \). The field \( \mathbb{Q}_p \) of \( p \)-adic numbers is the completion of \( \mathbb{Q} \) with respect to \( d_p \). We have a canonical metric, call it again \( d_p \), on \( \mathbb{Q}_p \) which extends the
previous one on $\mathbb{Q} \subset \mathbb{Q}_p$ (this inclusion is given by sending $a \in \mathbb{Q}$ to the constant Cauchy sequence $a,a,\ldots$). The same construction with the usual norm of $\mathbb{Q}$, i.e. $d(a,b) = |a - b|$ yields to the field of real numbers $\mathbb{R}$.

**Exercise 77** Prove that the two definitions of $\mathbb{Q}_p$ presented above are equivalent. Prove also

$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\} = \text{the closure of } \mathbb{Z} \text{ in } \mathbb{Q}_p$
Chapter 11
Theta series

Jacobi’s theta function is the following infinite sum

\[ \theta(z, \tau) = \sum_{n=-\infty}^{\infty} e^{2\pi inz + \pi in^2 \tau} \]

**Proposition 11.0.1** The Jacobi’s theta function satisfies:

1. It is a holomorphic function in \( \mathbb{C} \times \mathbb{H} \)
2. \( \theta(z + 1, \tau) - \theta(z, \tau) \)
3. \( \theta(z + \tau, \tau) - \theta(z, \tau) e^{-\pi i \tau} e^{-2\pi i \tau} \)
4. \( \theta(z, \tau) = 0 \) for \( z = \frac{1}{2} + \frac{\tau}{2} + n + m\tau, \ n, m \in \mathbb{Z} \)

**Proof.**

1. For \( |z| < M \) and \( \text{Im}(\tau) > 0 \) we have

\[
\sum_{n=-\infty}^{\infty} \left| e^{2\pi inZ + \pi in^2 \tau} \right| \leq C \sum_{n=0}^{\infty} e^{2\pi nM} e^{-\pi n^2 \tau_0}
\]

for some \( C \in \mathbb{R}^+ \). This shows that \( \theta \) is converges is \( \mathbb{C} \times \mathbb{H} \).

2. This is immediate

3.

\[
\theta(z + \tau, \tau) = \sum_{n=-\infty}^{\infty} e^{2\pi inz} e^{\pi i (n^2 + 2n) \tau}
\]

\[
= \sum_{n=-\infty}^{\infty} e^{2\pi i (n+1) z} e^{\pi i (n+1)^2 \tau} e^{-\pi i \tau} e^{-2\pi i \tau}
\]

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

4.

\[
\theta \left( \frac{1}{2} + \frac{\tau}{2}, \tau \right) = \sum_{n=-\infty}^{\infty} (-1)^n e^{\pi i (n^2 + n) \tau}
\]

For \( n \geq 0 \) the terms corresponding to \( n \) and \( -n - 1 \) cancel each other.
We will frequently use the followings:

\[ \theta_3(\tau) = \theta(0, \tau) \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}n^2} \]
\[ \theta_4(\tau) = \theta\left(\frac{1}{2}, \tau\right) \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}n^2} \]
\[ \theta_2(\tau) = \theta\left(\tau^2, \tau\right) = q^{-\frac{1}{4}} \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}(n+\frac{1}{2})^2} \]

**Theorem 11.0.1** We have

\[ \theta(z, \tau) = \prod_{n=1}^{\infty} \left( 1 - q^n \right) \left( 1 + q^{n-\frac{1}{2}} e^{2\pi i z} \right) \left( 1 + q^{n-\frac{1}{2}} e^{-2\pi i z} \right) \quad (11.1) \]

**Proof.** Let \( \pi(z, \tau) \) be the right hand side of (11.1). We prove that \( \pi(z, \tau) \) is a holomorphic function in \( \mathbb{C} \times \mathbb{H} \) and satisfies the same properties as of \( \theta(z, \tau) \) in

1. For the convergence we use the criterion for convergence of infinite products.

\[ (1 - q^n) \left( 1 - q^{n-\frac{1}{2}} e^{2\pi i z} \right) \left( 1 - q^{n-\frac{1}{2}} e^{-2\pi i z} \right) = 1 + O \left( |9|^{n-1} e^{2\pi i |z|} \right) \]

and \( \sum_{n=1}^{\infty} |9|^n \) converges.

2. This is immediate

3. \[ \pi(z, \tau) = \prod_{n=1}^{\infty} \left( 1 - q^n \right) \left( 1 - q^{n+\frac{1}{2}} e^{2\pi i z} \right) \left( 1 - q^{n-\frac{1}{2}} e^{-2\pi i z} \right) \]
\[ = \frac{(1 - q^{-\frac{1}{2}} e^{-2\pi i z})}{(1 - q^{\frac{1}{2}} e^{2\pi i z})} \pi(z, \tau) \]

We have \( \frac{1 + \chi}{1 + \chi^{-1}} = \chi, \chi \neq -1 \) and 3 follows.

4. The product vanishes at a point \((z, \tau)\) if

\[ \pm Z + \left( n - \frac{1}{2} \right) \tau \in \mathbb{Z} + \frac{1}{2} \]

which gives us the result.

Now, let us prove the equality (11.1) Let \( F(z, \tau) = \frac{\theta(z, \tau)}{\pi(z, \tau)} \). This as a function in \( z \) is double periodic and has no poles. Therefore, it is constant as a function in \( z \). Therefore \( C(\tau) = \theta(z, \tau)/\pi(z, \tau) \).

We put \( z = \frac{1}{2} \)
\[ C(\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2} n^2} \prod_{n=1}^{\infty} \left( 1 - q^{4n} \right) \left( 1 - q^{8n-2} \right) \] (11.2)

We put \( z = \frac{1}{4} \)

\[ C(\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{2n^2} \prod_{n=1}^{\infty} \left( 1 - q^{2n} \right) \left( 1 - q^{4n-2} \right) \] (11.3)

11.2 and 11.3 imply \( C(4\tau) = C(\tau) \) for all \( \tau \in \mathbb{H} \). Since \( q^{4k} \to 0 \) when \( k \to \infty \) we can conclude that \( C(\tau) = 1 \)

We have

\[ \theta_3(\tau) = \frac{\eta(\tau)^5}{\eta \left( \frac{1}{2} \tau \right)^2 \eta(2\tau)^2} \] (11.4)

\[ \theta_4(\tau) = \frac{\eta \left( \frac{1}{2} \tau \right)^2}{\eta(\tau)} \] (11.5)

\[ \theta_2(\tau) = \frac{2\eta(2\tau)^2}{\eta(\tau)} \] (11.6)

Taken from Wikipedia and [Oliver]. Note that \( \theta_2 \theta_3 \theta_4 = 2 \eta(\tau)^3 \).

**Theorem 11.0.2** For \( \tau \in \mathbb{H} \) and \( z \in \mathbb{C} \) we have

\[ \theta \left( z, \frac{-1}{\tau} \right) = \sqrt{\frac{\tau}{i}} e^{\pi i z^2} \theta(z\tau, \tau) \]

Here we have chosen a branch of \( \sqrt{\tau} \), \( \tau \in \mathbb{H} \) such that for imaginary \( \tau \), it is positive.

**Proof.** It is enough to prove the formula \( z = \alpha \in \mathbb{R} \) and \( \tau = it, t \in \mathbb{R}^+ \). This is exactly the Poisson summation formula.

We get the following functional equations for \( \theta_2, \theta_3, \theta_4 \)

\[ \theta_3 \left( \frac{-1}{\tau} \right) = \sqrt{\frac{\tau}{i}} \theta_3(\tau) \] (11.7)

\[ \theta_4 \left( \frac{-1}{\tau} \right) = \sqrt{\frac{\tau}{i}} \xi_8 \cdot \theta_2(\tau) \]

\[ \eta \left( \frac{-1}{\tau} \right) = \sqrt{\frac{\tau}{i}} \cdot \eta(\tau) \]
Let \( f(\tau) = \theta_3(8\tau)^8 \)

\[
\begin{align*}
lf(\tau + 1) &= f(\tau) \\
f\left(\frac{-1}{4\tau}\right) &= \left(\frac{\tau}{2}\right)^4 f(\tau)
\end{align*}
\]

Which says that \( f \) is a modular form for the group

\[
\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 21 & 2 \end{pmatrix} \rangle \subseteq \text{SL}(2, \mathbb{Q})
\]

### 11.1 Two-squares theorem

For \( k \in \mathbb{N} \), \( a = (a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k \)

\[
\gamma_k, a(n) = \# \{ (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k | a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2 = n \}
\]

Then

\[
\theta(2a_1 \tau) \theta(2a_2 \tau) \cdots \theta(2a_k \tau) = \sum_{n=0}^{\infty} \gamma_k, a(n) q^n. \tag{11.8}
\]

Therefore, in order to find formulas for \( \gamma_k, a(n) \) we have to study the analytic function in the left hand side of \(11.8\).

Let \( d_1(n) \) denotes the number of divisors of \( n \) of the form \( 4k + 1 \), and \( d_3(n) \) the number of divisors of \( n \) of the form \( 4k + 3 \).

**Theorem 11.1.1** For \( n \geq 1 \)

\[
\gamma_2(n) = 4 \left( d_1(n) - d_3(n) \right) \tag{11.9}
\]

The generating function of the right hand side of \(11.9\) is

\[
C(\tau) = 2 \sum_{n=-\infty}^{+\infty} \frac{1}{q^n + q^{-n}} = 1 + 4 \sum_{n=1}^{\infty} \frac{q^n}{1 + q^{4n}} = 1 + 4 \sum_{n=1}^{\infty} \frac{q^n}{1 - q^{4n}} - \frac{q^{3n}}{1 - q^{4n}}
\]

Therefore, in order to prove \(11.1.1\) we have to prove that

\[
\theta_3^2(2\tau) = C(\tau)
\]
For the rest of the proof see [Stein] page 299.

11.2 Poisson summation formula

Let \( \varphi : \mathbb{R} \to \mathbb{R} \) be any continuous function which decreases rapidly, let us say

\[
\varphi(x) \sim |x|^{-c} \quad c > 0
\]

as \( x \to +\infty \). Then the Fourier transform of \( \varphi \) is

\[
\hat{\varphi}(y) := \int_{\mathbb{R}} \varphi(x) e^{-2\pi i xy} \, dx
\]

The Poisson summation formula says that

\[
\sum_{n \in \mathbb{Z}} \varphi(x+n) = \sum_{\gamma \in \mathbb{Z}} \hat{\varphi}(x+\gamma)
\]  \hspace{1cm} (11.10)

**Proof.** (Taken from Zagier) The growth condition on \( \varphi(x) \) ensures that the left hand side of (11.10) converges to a continuous function \( \Phi \). This function satisfies

\[
\Phi(x+1) = \Phi(x)
\]

and so \( \Phi \) has Fourier expansion

\[
\Phi(x) = \sum_{\gamma \in \mathbb{Z}} c_{\gamma} e^{2\pi i \gamma x} \quad c_{\gamma} = \int_{0}^{1} \Phi(x) e^{-2\pi i \gamma x} \, dx
\]

Substituting \( c_{\gamma} \) in \( \Phi(x) \) we get

\[
c_{\gamma} = \int_{0}^{1} \sum_{n=-\infty}^{\infty} \varphi(x+n) e^{-2\pi i \gamma (x+n)} \, dx = \sum_{n=-\infty}^{\infty} \int_{n}^{n+1} \varphi(x) e^{-2\pi i \gamma x} \, dx = \int_{-\infty}^{\infty} \varphi(x) e^{-2\pi i \gamma x} \, dx
\]

This gives us

\[
\sum_{n \in \mathbb{Z}} \varphi(x+n) = \sum_{\gamma \in \mathbb{Z}} \left( \int_{\mathbb{R}} \varphi(t) e^{-2\pi i \gamma t} \, dt \right) e^{2\pi i \gamma x}
\]

which is the desired statement. \( \blacksquare \)
In this section we reproduce an example of a foliation, see Theorem 12.2, which is essentially due to E. Picard in [Pic89] pages 298-299, see also Mazzocco’s article [Maz01]. Picard has taken an evaluation of the Weierstrass \( \wp \) function to give a solution to Painlevé VI equation with a particular parameter, see also Corollary 2 and 3 in [Lor16]. This particular case of Painlevé VI written as a vector field is birational to the foliation in Theorem 12.2. We have derived Picard’s foliation using the Gauss-Manin connection of half elliptic integrals and in this way its generalization to families of curves of arbitrary genus is reachable.

Let \( T \) be the moduli of triples \((E, \omega, P)\), where \( E \) is an elliptic curve, \( \omega \) is a holomorphic differential form on \( E \) and \( P \) is a point in \( E \) with \( P \neq O \). Note that in this text an elliptic curve comes with a point \( O \) which is the neutral point of the group structure of \( E \). This is almost the same moduli as F. Loray’s moduli space in [Lor16]. We take the line bundle \( L = [P] - [O] \), which automatically comes with the divisor \( P - O \). The connection \( \nabla : L \to \Omega^1_E \otimes L \) is determined by \( \nabla s = \omega \otimes s \). Loray in [Lor16] works with the Legendre family which the moduli elliptic curves with a 2-torsion point structure, whereas in our context we do not consider this.

The universal family of pairs \((E, \omega)\) is given by the Weierstrass family

\[
E_{t_2,t_3}, \quad y^2 = 4x^3 - t_2x - t_3, \quad \omega = \frac{dx}{y}, \quad (t_2,t_3) \in \mathbb{C}^2 \setminus \{27t_3^2 - 4t_2 = 0\} \tag{12.1}
\]

and for a given \((E, \omega)\), its Weierstrass coordinates \((x, y)\) are unique. We have four functions

\[
t_2, t_3, \quad \tilde{x} := x(P), \quad \tilde{y} := y(P)
\]

on \( T \) which satisfy the relation (12.1). We may choose \((\tilde{x}, \tilde{y}, t_2)\) as coordinate system on \( T \). On \( T \) we have the following holomorphic multi-valued functions

\[
\int_{\tilde{O}} \alpha, \int_{\tilde{\delta}_1} \alpha, \int_{\tilde{\delta}_2} \alpha \tag{12.2}
\]
where \( \delta_1, \delta_2 \in H_1(E, \mathbb{Z}) \) form a basis and varies continously when \( E \) changes in the moduli space (flat sections of the Gauss-Manin connection after going to \( H^1 \)), and \( \alpha = \left( \frac{dx}{y}, \frac{dy}{y} \right) \).

**Theorem 12.0.1** There is a unique algebraic one dimensional foliation \( \mathbb{F} \) in \( T \) such that

1. The three vector valued holomorphic functions \([12.2]\) restricted to the leaves of \( \mathbb{F} \) are linearly dependent (with constant coefficients depending only on the leaf \( L \)).

2. The foliation \( \mathbb{F} \) has the first integral \( f := \frac{y^2}{t^2} \).

3. The foliation \( \mathbb{F} \) has an enumerable set of algebraic leaves birationl to mod-ular curves, we denote them by \( X_0(d), d \in \mathbb{N}, d \geq 2 \). There is a sequence \( c_2, c_3, \cdots, c_d, \cdots \in \mathbb{C} \cup \{ \infty \} \) with \( c_2 = \infty \) such that \( X_0(d) \subset f^{-1}(c_d) \) and the point \( (E, \infty, P) \) of \( X_0(d) \) is characterized by the fact that \( P \) is a torsion point of order \( d \) in \( E \).

4. The foliation \( \mathbb{F} \) is given by the vector field

\[
y \left( \frac{2}{3} t^2 \frac{\partial}{\partial t^2} + t_3 \frac{\partial}{\partial t_3} - y^2 (6x^2 t_2 - t_2^2 + 9x t_3) \frac{\partial}{\partial x} \right) + \left( y^2 (\frac{3}{2} t_2 - 6x^2) (6x^2 t_2 - t_2^2 + 9x t_3) - \frac{1}{3} t_2 x - \frac{1}{2} t_3 \right) \frac{\partial}{\partial y} \tag{12.3}
\]

\[
\left( y^2 (\frac{3}{2} t_2 - 6x^2) (6x^2 t_2 - t_2^2 + 9x t_3) - \frac{1}{3} t_2 x - \frac{1}{2} t_3 \right) \frac{\partial}{\partial y} \tag{12.4}
\]

Picard’s foliation has the following singular set

\[
\text{Sing}(\mathbb{F}) := \{ t_2 = y^2 - 4x^3 = 0 \} \cup \{ x = y = 0 \} \cup \{ y = 12t_2 - x^2 = 0 \} \tag{12.5}
\]

**Proof.** In the following \( d \) refers to differential operator in \( T \) space. We have the following differential equation

\[
\begin{pmatrix}
\frac{d}{y} \left( \int_0^y \frac{dx}{y} \right) \\
\frac{d}{y} \left( \int_0^y dx \right)
\end{pmatrix} = \begin{pmatrix}
-\frac{1}{12} \frac{\partial}{\partial \alpha}, & 3 \frac{\partial}{\partial \alpha} \\
-\frac{1}{8} \frac{\partial}{\partial \beta}, & \frac{1}{12} \frac{\partial}{\partial \beta}
\end{pmatrix} \begin{pmatrix}
\int_0^y \frac{dx}{y} \\
\int_0^y ydx
\end{pmatrix} + \begin{pmatrix}
A_1(\beta, \gamma) + \frac{dx}{y} \\
A_2(\beta, \gamma) + \frac{dx}{y}
\end{pmatrix} \tag{12.6}
\]

where

\[
\Delta := 27t_2^2 - t_3^3, \quad \alpha := 3t_3 dt_2 - 2t_2 dt_3.
\]

\[
A_1 = (9x^2 y - \frac{3}{2} t_2 y) dt_2 + (9xy) dt_3
\]

\[
A_2 = (18x^3 y - \frac{9}{4} y^3 - \frac{15}{4} t_2 xy) dt_2 + (9x^2 y - \frac{3}{2} t_2 y) dt_3
\]

The full periods \( \int_0^y \alpha \) satisfy the above differential equations without the last term. In this case the involving \( 2 \times 2 \) matrix in \( t_2, t_3 \) variables is usually called the Gauss-Manin connection matrix of the family \([12.1]\). The computation of this matrix can
be found in [Sas74] p. 304, [Sat01]. For the algorithms which computes the Gauss-Manin connections in other cases, and in particular, the computation of the last term in the above equality see [Mov19].

We are looking for a foliation with the first property in Theorem 12.2. This is given by the two differential forms in the last matrix of (12.6). The vector field in the theorem generates the common kernel of these 1-forms.
Chapter 13
Online supplemental items

13.1 Introduction

In this chapter we explain many procedures of the library foliation.lib of Singular, [GPS01], a computer programming language for polynomial computations. We also explain few other softwares which are useful when one deal with computational aspects of modular forms and elliptic curves.

13.2 How to start?

One has to run Singular in the same directory, where foliation.lib lies. Then in Singular’s command line one has to type:

```
LIB "foliation.lib";
```

In order to get an example and help of a command, for instance PeriodMatrix, one has to type respectively:

```
example PeriodMatrix;
help PeriodMatrix;
```

In this chapter I will only sketch few procedures related to the topic of the present text. For more information the reader might consult the help and example of each procedure.

13.3 Ramanujan differential equation
References


## Index

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, lattice</td>
<td>9</td>
</tr>
<tr>
<td>$\tau$, coordinate in the upper half plane</td>
<td>9</td>
</tr>
<tr>
<td>Dedekind eta function</td>
<td>6</td>
</tr>
<tr>
<td>Elliptic curve</td>
<td>37</td>
</tr>
<tr>
<td>Elliptic function</td>
<td>12</td>
</tr>
<tr>
<td>Lattice</td>
<td>9</td>
</tr>
<tr>
<td>Lattice of elliptic integrals</td>
<td>38</td>
</tr>
<tr>
<td>Modular form</td>
<td>12</td>
</tr>
<tr>
<td>Point at infinity</td>
<td>37</td>
</tr>
<tr>
<td>Serre derivative</td>
<td>24</td>
</tr>
<tr>
<td>Weierstrass form</td>
<td>37</td>
</tr>
</tbody>
</table>