Galois Representations and Automorphic Forms
(MasterMath)

Peter Bruin and Arno Kret

Autumn 2016

Preliminary draft; comments and corrections are welcome
# Contents

1 Introduction .......................... 2
   1.1 Quadratic reciprocity ............... 3
   1.2 First examples of $L$-functions ... 5
   1.3 Modular forms and elliptic curves ... 11
   1.4 More examples of $L$-functions ... 14
   1.5 Exercises ................................ 18
Chapter 1

Introduction

Contents

1.1 Quadratic reciprocity ........................................... 3
1.2 First examples of \(L\)-functions ................................. 5
  1.2.1 The Riemann \(\zeta\)-function ............................... 5
  1.2.2 Dedekind \(\zeta\)-functions ................................ 8
  1.2.3 Dirichlet \(L\)-functions .................................. 9
  1.2.4 An example of a Hecke \(L\)-function ..................... 10
1.3 Modular forms and elliptic curves ............................ 11
  1.3.1 Elliptic curves ............................................. 11
  1.3.2 Modular forms ............................................. 13
1.4 More examples of \(L\)-functions ................................. 14
  1.4.1 Artin \(L\)-functions ........................................ 14
  1.4.2 \(L\)-functions attached to elliptic curves ............... 16
  1.4.3 \(L\)-functions attached to modular forms ............... 17
1.5 Exercises ....................................................... 18

In this first chapter, our main goal will be to motivate why one would like to study the objects that this course is about, namely Galois representations and automorphic forms. We give two examples that will later turn out to be known special cases of the Langlands correspondence, namely Gauss’s quadratic reciprocity theorem and the modularity theorem of Wiles et al. We note that the general Langlands correspondence is still largely conjectural and drives much current research in number theory.

Along the way, we will encounter various number-theoretic objects, such as number fields, elliptic curves, modular forms and Galois representations, and we will associate \(L\)-functions to them. These will turn out to form the link by which one can relate objects (such as elliptic curves and modular forms) that a priori seem to be very different.
1.1 Quadratic reciprocity

Recall that if \( p \) is a prime number, then the Legendre symbol modulo \( p \) is defined, for all \( a \in \mathbb{Z} \), by

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^*, \\
-1 & \text{if } a \text{ is a non-square in } (\mathbb{Z}/p\mathbb{Z})^*, \\
0 & \text{if } a \text{ is congruent to } 0 \text{ modulo } p. 
\end{cases}
\]

**Theorem 1.1 (Quadratic reciprocity law).** Let \( p \) and \( q \) be two distinct odd prime numbers. Then

\[
\left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

To put this in the context of this course, we consider two different objects. The first object (a Dirichlet character) lives in the “automorphic world”, the second (a character of the Galois group of a number field) lives in the “arithmetic world”.

On the one hand, consider the quadratic Dirichlet character

\[ \chi_q : (\mathbb{Z}/q\mathbb{Z})^* \to \{ \pm 1 \} \]

defined by the Legendre symbol

\[ \chi_q(a \mod q) = \left( \frac{a}{q} \right). \]

From the fact that the subgroup of squares has index 2 in \( (\mathbb{Z}/q\mathbb{Z})^* \), it follows that \( \chi_q \) is a surjective group homomorphism.

On the other hand, we consider the field

\[ K_q = \mathbb{Q}(\sqrt{q^*}) \]

where \( q^* = (-1)^{(q-1)/2}q \). The Galois group \( \text{Gal}(K_q/\mathbb{Q}) \) has order 2 and consists of the identity and the automorphism \( \sigma \) defined by \( \sigma(\sqrt{q^*}) = -\sqrt{q^*} \).

To any prime \( p \neq q \) we associate a Frobenius element

\[ \text{Frob}_p \in \text{Gal}(K_q/\mathbb{Q}). \]

The general definition does not matter at this stage; it suffices to know that

\[ \text{Frob}_p = \begin{cases} 
\text{id} & \text{if } p \text{ splits in } K_q, \\
\sigma & \text{if } p \text{ is inert in } K_q. 
\end{cases} \]

Furthermore, there exists a (unique) isomorphism

\[ \epsilon_q : \text{Gal}(K_q/\mathbb{Q}) \xrightarrow{\sim} \{ \pm 1 \}. \]

By definition, a prime \( p \in \mathbb{Z} \) splits in \( K_q \) if and only if \( q^* \) is a square modulo \( p \); in other words, we have

\[ \epsilon_q(\text{Frob}_p) = \left( \frac{q^*}{p} \right). \]
Note that
\[
\left( \frac{q^*}{p} \right) = \left( \frac{-1}{p} \right)^{(q-1)/2} \left( \frac{q}{p} \right)
\]
and
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2},
\]
so the quadratic reciprocity law is equivalent to
\[
\left( \frac{q^*}{p} \right) = \left( \frac{p}{q} \right),
\]
which is in turn equivalent to
\[
\epsilon_q(Frob_p) = \chi_q(p \mod q).
\]

Note that it is not at all obvious that the splitting behaviour of a prime \( p \) in \( K_q \) only depends on a congruence condition on \( p \).

**Sketch of proof of the quadratic reciprocity law.** The proof uses the cyclotomic field \( \mathbb{Q}(\zeta_q) \).

It is known that this is an Abelian extension of degree \( \phi(q) = q - 1 \) of \( \mathbb{Q} \), and that there exists an isomorphism
\[
(\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})
\]
\[
a \mapsto \sigma_a,
\]
where \( \sigma_a \) is the unique automorphism of the field \( \mathbb{Q}(\zeta_q) \) with the property that \( \sigma_a(\zeta_q) = \zeta_q^a \).

There is a notion of Frobenius elements \( \text{Frob}_p \in \mathbb{Q}(\zeta_q) \) for every prime number \( p \) different from \( q \), and we have
\[
\sigma_{p \mod q} = \text{Frob}_p.
\]

In Exercise (1.6), you will prove that there exists an embedding of number fields
\[
K_q \hookrightarrow \mathbb{Q}(\zeta_q).
\]

Such an embedding (there are two of them) induces a surjective homomorphism between the Galois groups. We consider the diagram
\[
\begin{array}{ccc}
\text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) & \longrightarrow & \text{Gal}(K_q/\mathbb{Q}) \\
\sim & & \sim \\
(\mathbb{Z}/q\mathbb{Z})^\times & \xrightarrow{\chi_q} & \{\pm 1\}.
\end{array}
\]

Since the group \( (\mathbb{Z}/q\mathbb{Z})^\times \) is cyclic, there exists exactly one surjective group homomorphism \( (\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\} \), so we see that the diagram is commutative. Furthermore, the map on Galois groups respects the Frobenius elements on both sides. Computing the image of \( p \) in \( \{\pm 1\} \) via the two possible ways in the diagram, we therefore conclude that
\[
\epsilon_q(Frob_p) = \chi_q(p \mod q),
\]
which is the identity that we had to prove. \( \square \)
1.2 First examples of \( L \)-functions

1.2.1 The Riemann \( \zeta \)-function

The prototypical example of an \( L \)-function is the \textit{Riemann \( \zeta \)-function}. It can be defined in (at least) two ways: as a \textit{Dirichlet series}

\[
\zeta(s) = \sum_{n \geq 1} n^{-s}
\]

or as an \textit{Euler product}

\[
\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.
\]

Both the sum and the product converge absolutely and uniformly on subsets of \( \mathbb{C} \) of the form \{\( s \in \mathbb{C} \mid \Re s \geq \sigma \} \) with \( \sigma > 1 \). Both expressions define the same function because of the geometric series identity

\[
\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \quad \text{for } |x| < 1
\]

and because every positive integer has a unique prime factorisation.

We define the \textit{completed \( \zeta \)-function} by

\[
Z(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).
\]

Here we have used the \( \Gamma \)-function, defined by

\[
\Gamma(s) = \int_0^\infty \exp(-t)t^{s-1} dt \quad \text{for } \Re s > 0.
\]

By repeatedly using the functional equation

\[
\Gamma(s + 1) = s\Gamma(s),
\]

one shows that the \( \Gamma \)-function can be continued to a meromorphic function on \( \mathbb{C} \) with simple poles at the non-positive integers and no other poles.

\textbf{Theorem 1.2} (Riemann, 1859). \textit{The function \( Z(s) \) can be continued to a meromorphic function on the whole complex plane with a simple pole at \( s = 1 \) with residue 1, a simple pole at \( s = 0 \) with residue \( -1 \), and no other poles. It satisfies the functional equation}

\[
Z(s) = Z(1 - s).
\]

\textit{Proof.} (We omit some details related to convergence of sums and integrals.) The proof is based on two fundamental tools: the \textit{Poisson summation formula} and the \textit{Mellin transform}. The Poisson summation formula says that if \( f: \mathbb{R} \to \mathbb{C} \) is smooth and quickly decreasing, and we define the Fourier transform of \( f \) by

\[
\hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi i xy) dx,
\]
then we have
\[ \sum_{m \in \mathbb{Z}} f(x + m) = \sum_{n \in \mathbb{Z}} \hat{f}(n) \exp(2\pi inx). \]
(This can be proved by expanding the left-hand side in a Fourier series and showing that this yields the right-hand side.) In particular, putting \( x = 0 \), we get
\[ \sum_{m \in \mathbb{Z}} f(m) = \sum_{n \in \mathbb{Z}} \hat{f}(n). \]
For fixed \( t > 0 \), we now apply this to the function
\[ f_t(x) = \exp(-\pi t^2 x^2). \]
By Exercise [1.7], the Fourier transform of \( f_t \) is given by
\[ \hat{f}_t(y) = t^{-1} \exp(-\pi y^2/t^2). \]
The Poisson summation formula gives
\[ \sum_{m \in \mathbb{Z}} \exp(-\pi m^2 t^2) = t^{-1} \sum_{n \in \mathbb{Z}} \exp(-\pi n^2/t^2). \]
Hence, defining the function
\[ \phi: (0, \infty) \rightarrow \mathbb{R} \quad t \mapsto \sum_{m \in \mathbb{Z}} \exp(-\pi m^2 t^2), \]
we obtain the relation
\[ \phi(t) = t^{-1} \phi(1/t). \tag{1.1} \]
The definition of \( \phi(t) \) implies
\[ \phi(t) \to 1 \quad \text{as} \quad t \to \infty, \]
and combining this with the relation \( \phi(t) \sim t^{-1} \) between \( \phi(t) \) and \( \phi(1/t) \) gives
\[ \phi(t) \sim t^{-1} \quad \text{as} \quad t \to 0. \]
To apply the Mellin transform, we need a function that decreases at least polynomially as \( t \to \infty \). We therefore define the auxiliary function
\[ \phi_0(t) = \phi(t) - 1 = 2 \sum_{m=1}^{\infty} \exp(-\pi m^2 t^2). \]
Then we have
\[ \phi_0(t) \sim t^{-1} \quad \text{as} \quad t \to 0 \]
and
\[ \phi_0(t) \sim 2 \exp(-\pi t^2) \quad \text{as} \quad t \to \infty. \]
Furthermore, the equation \( \phi(t) \sim t^{-1} \) implies
\[ \phi_0(t) = t^{-1} \phi_0(1/t) + t^{-1} - 1. \tag{1.2} \]
CHAPTER 1. INTRODUCTION

Next, we consider the Mellin transform of $\phi_0$, defined by

$$(\mathcal{M}\phi_0)(s) = \int_0^\infty \phi_0(t) t^s \frac{dt}{t}. $$

Due to the asymptotic behaviour of $\phi_0(t)$, the integral converges for $\Re s > 1$. We will now rewrite $(\mathcal{M}\phi_0)(s)$ in two different ways to prove the analytic continuation and functional equation of $Z(s)$.

On the one hand, substituting the definition of $\phi_0(t)$, we obtain

$$(\mathcal{M}\phi_0)(s) = 2 \int_0^\infty \left( \sum_{n=1}^\infty \exp(-\pi n^2 t^2) \right) t^s \frac{dt}{t}$$

Making the change of variables $u = \pi n^2 t^2$ in the $n$-th term, we obtain

$$(\mathcal{M}\phi_0)(s) = \sum_{n=1}^\infty \int_0^\infty \exp(-u) \left( \frac{u}{\pi n^2} \right)^{s/2} \frac{du}{u}$$

$$= \frac{\Gamma(s/2)}{\pi^{s/2}} \zeta(s) = Z(s).$$

On the other hand, we can split up the integral defining $(\mathcal{M}\phi_0)(s)$ as

$$(\mathcal{M}\phi_0)(s) = \int_0^1 \phi_0(t) t^s \frac{dt}{t} + \int_1^\infty \phi_0(t) t^s \frac{dt}{t}.$$Substituting $t = 1/u$ in the first integral and using (1.2), we get

$$\int_0^1 \phi_0(t) t^s \frac{dt}{t} = \int_1^\infty \phi_0(1/u) u^{-s} \frac{du}{u}$$

Using the identity $\int_1^\infty u^{-a} \frac{du}{u} = 1/a$ for $\Re a > 0$, we conclude

$$(\mathcal{M}\phi_0)(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(t) t^s dt + \int_1^\infty \phi_0(t) t^{1-s} dt.$$From the two expressions for $(\mathcal{M}\phi_0)(s)$ obtained above, both of which are valid for $\Re s > 1$, we conclude that $Z(s)$ can be expressed for $\Re s > 1$ as

$$Z(s) = (\mathcal{M}\phi_0)(s)$$

$$= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(t) t^s dt + \int_1^\infty \phi_0(t) t^{1-s} dt.$$Both integrals converge for all $s \in \mathbb{C}$. The right-hand side therefore gives the meromorphic continuation of $Z(s)$ with the poles described in the theorem. Furthermore, it is clear that the right-hand side is invariant under the substitution $s \mapsto 1-s$. \qed
Remark 1.3. Each of the above two ways of writing $\zeta(s)$ (as a Dirichlet series or as an Euler product) expresses a different aspect of $\zeta(s)$. The Dirichlet series is needed to obtain the analytic continuation, while the Euler product highlights the relationship to the prime numbers.

### 1.2.2 Dedekind $\zeta$-functions

The Riemann $\zeta$-function expresses information related to arithmetic in the rational field $\mathbb{Q}$. Next, we go from $\mathbb{Q}$ to general number fields (finite extensions of $\mathbb{Q}$). We will introduce Dedekind $\zeta$-functions, which are natural generalisations of the Riemann $\zeta$-function to arbitrary number fields.

Let $K$ be a number field, and let $\mathcal{O}_K$ be its ring of integers. For every non-zero ideal $a$ of $\mathcal{O}_K$, the norm of $a$ is defined as $N(a) = \#(\mathcal{O}_K/a)$.

**Definition 1.4.** Let $K$ be a number field. The Dedekind $\zeta$-function of $K$ is the function $\zeta_K: \{s \in \mathbb{C} \mid \Re s > 1\} \to \mathbb{C}$ defined by

$$\zeta_K(s) = \sum_{a \subseteq \mathcal{O}_K} N(a)^{-s},$$

where $a$ runs over the set of all non-zero ideals of $\mathcal{O}_K$.

By unique prime ideal factorisation in $\mathcal{O}_K$, we can write

$$\zeta_K(s) = \prod_p \frac{1}{1 - N(p)^{-s}},$$

where $p$ runs over the set of all non-zero prime ideals of $\mathcal{O}_K$.

The same reasons why one should be interested the Riemann $\zeta$-function also apply to the Dedekind $\zeta$-function: its non-trivial zeroes encode the distribution of prime ideals in $\mathcal{O}_K$, while its special values encode interesting arithmetic data associated with $K$.

Let $\Delta_K \in \mathbb{Z}$ be the discriminant of $K$, and let $r_1$ and $r_2$ denote the number of real and complex places of $K$, respectively. Then one can show that the completed $\zeta$-function

$$Z_K(s) = |\Delta_K|^{s/2}(\pi^{-s/2}\Gamma(s/2))^{r_1}((2\pi)^{1-s}\Gamma(s))^{r_2}\zeta_K(s)$$

has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$Z_K(s) = Z_K(1 - s).$$

**Theorem 1.5** (Class number formula). Let $K$ be a number field. In addition to the above notation, let $h_K$ denote the class number, $R_K$ the regulator, and $w_K$ the number of roots of unity in $K$. Then $\zeta_K(s)$ has a simple pole in $s = 1$ with residue

$$\text{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_KR_K}{|\Delta_K|^{1/2}w_K}.$$

Furthermore, one has

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}} = -\frac{h_KR_K}{w_K}.$$
1.2.3 Dirichlet $L$-functions

Next, we will describe a construction of $L$-functions that is of a somewhat different nature, since it does not directly involve number fields or Galois theory. Instead, it is more representative of the $L$-functions that we will later attach to automorphic forms.

**Definition 1.6.** Let $n$ be a positive integer. A Dirichlet character modulo $n$ is a group homomorphism

$$
\chi: (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*.
$$

Let $n$ be a positive integer, and let $\chi$ be a Dirichlet character modulo $n$. We extend $\chi$ to a function

$$
\tilde{\chi}: \mathbb{Z} \to \mathbb{C}
$$

by putting

$$
\tilde{\chi}(m) = \begin{cases} 
\chi(m \mod n) & \text{if } \gcd(m, n) = 1, \\
0 & \text{if } \gcd(m, n) > 1.
\end{cases}
$$

By abuse of notation, we will usually write $\chi$ for $\tilde{\chi}$. Furthermore, we let $\bar{\chi}$ denote the complex conjugate of $\chi$, defined by

$$
\bar{\chi}: \mathbb{Z} \to \mathbb{C},
$$

$$
\bar{\chi}(m) = \overline{\chi(m)}.
$$

One checks immediately that $\tilde{\chi}$ is a Dirichlet character satisfying

$$
\chi(m)\bar{\chi}(m) = \begin{cases} 
1 & \text{if } \gcd(m, n) = 1, \\
0 & \text{if } \gcd(m, n) > 1.
\end{cases}
$$

For fixed $n$, the set of Dirichlet characters modulo $n$ is a group under pointwise multiplication, with the identity element being the trivial character modulo $n$ and the inverse of $\chi$ being $\bar{\chi}$. This group can be identified with $\text{Hom}((\mathbb{Z}/n\mathbb{Z})^*, \mathbb{C}^*)$. It is non-canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, and its order is $\phi(n)$, where $\phi$ is Euler’s $\phi$-function.

Let $n, n'$ be positive integers with $n \mid n'$, and let $\chi$ be a Dirichlet character modulo $m$. Then $\chi$ can be lifted to a Dirichlet character $\chi^{(n')}$ modulo $n'$ by putting

$$
\chi^{(n')}(m) = \begin{cases} 
\chi(m) & \text{if } \gcd(m, n') = 1, \\
0 & \text{if } \gcd(m, n') > 1.
\end{cases}
$$

The conductor of a Dirichlet character $\chi$ modulo $n$ is the smallest divisor $n_\chi$ of $n$ such that there exists a Dirichlet character $\chi_0$ modulo $n_\chi$ satisfying $\chi = \chi_0^{(n)}$. A Dirichlet character $\chi$ modulo $n$ is called primitive if $n_\chi = n$.

**Remark 1.7.** If you already know about the topological ring $\hat{\mathbb{Z}} = \lim_{\leftarrow n \geq 1} \mathbb{Z}/n\mathbb{Z}$ of profinite integers, you may alternatively view a Dirichlet character as a continuous group homomorphism

$$
\chi: \hat{\mathbb{Z}}^* \to \mathbb{C}^*.
$$

This is a first step towards the notion of automorphic representations. Vaguely speaking, these are representations (in general infinite-dimensional) of non-commutative groups somewhat resembling $\hat{\mathbb{Z}}^*$. 
Note that when we view Dirichlet characters as homomorphisms $\chi: \hat{\mathbb{Z}}^\times \to \mathbb{C}^\times$, there is no longer a notion of a modulus of $\chi$. However, we can recover the conductor of $\chi$ as the smallest positive integer $n_\chi$ for which $\chi$ can be factored as a composition

$$\chi: \hat{\mathbb{Z}}^\times \to (\mathbb{Z}/n_\chi \mathbb{Z})^\times \to \mathbb{C}^\times.$$ 

**Definition 1.8.** Let $\chi: \mathbb{Z} \to \mathbb{C}$ be a Dirichlet character modulo $n$. The Dirichlet $L$-function attached to $\chi$ is the function

$$L(\chi, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$ 

In a similar way as for the Riemann $\zeta$-function, one shows that the sum converges absolutely and uniformly on every right half-plane of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with $\sigma > 1$. This implies that the above Dirichlet series defines a holomorphic function $L(\chi, s)$ on the right half-plane $\{s \in \mathbb{C} \mid \Re s > 1\}$.

Furthermore, the multiplicativity of $L(\chi, s)$ implies the identity

$$L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}} \text{ for } \Re s > 1.$$ 

In Exercise 1.8 you will show that $L(\chi, s)$ admits an analytic continuation and functional equation similar to those for $\zeta(s)$.

**Remark 1.9.** The functions $L(\chi, s)$ were introduced by P. G. Lejeune-Dirichlet in the proof of his famous theorem on primes in arithmetic progressions:

**Theorem** (Dirichlet, 1837). Let $n$ and $a$ be coprime positive integers. Then there exist infinitely many prime numbers $p$ with $p \equiv a \pmod{n}$.

### 1.2.4 An example of a Hecke $L$-function

Just as Dedekind $\zeta$-functions generalise the Riemann $\zeta$-function, the Dirichlet $L$-functions $L(\chi, s)$ can be generalised to $L$-functions of Hecke characters. As the definition of Hecke characters is slightly involved, we just give an example at this stage.

Let $I$ be the group of fractional ideals of the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers. We define a group homomorphism

$$\chi: I \to \mathbb{Q}(\sqrt{-1})^\times$$

$$a \mapsto a^4,$$

where $a \in \mathbb{Q}(\sqrt{-1})$ is any generator of the fractional ideal $a$. Such an $a$ exists because $\mathbb{Z}[\sqrt{-1}]$ is a principal ideal domain, and is unique up to multiplication by a unit in $\mathbb{Z}[\sqrt{-1}]$. In particular, since all units in $\mathbb{Z}[\sqrt{-1}]$ are fourth roots of unity, $\chi(a)$ is independent of the choice of the generator $a$. Furthermore, we have $N(a) = |a|^2$. After choosing an embedding $\mathbb{Q}(\sqrt{-1}) \hookrightarrow \mathbb{C}$, we can view $\chi$ as a homomorphism $I \to \mathbb{C}^\times$. This is one of the simplest examples of a Hecke character.

We define a Dirichlet series $L(\chi, s)$ by

$$L(\chi, s) = \sum_a \chi(a) N(a)^{-s},$$
CHAPTER 1. INTRODUCTION

where \( a \) runs over all non-zero integral ideals of \( \mathbb{Z}[\sqrt{-1}] \), and where as before \( N(a) \) denotes the norm of the ideal \( a \). One can check that this converges for \( 4 - 2s < -2 \) and therefore defines a holomorphic function on \( \{ s \in \mathbb{C} \mid \Re s > 3 \} \). By unique ideal factorisation in \( \mathbb{Z}[\sqrt{-1}] \), this \( L \)-function admits an Euler product

\[
L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)N(p)^{-s}}
= \prod_{p \text{ prime}} \prod_{p | p} \frac{1}{1 - \chi(p)N(p)^{-s}}.
\]

where \( p \) runs over the set of all non-zero prime ideals of \( \mathbb{Z}[\sqrt{-1}] \).

Concretely, the ideals of smallest norm in \( \mathbb{Z}[\sqrt{-1}] \) and the values of \( \chi \) on them are

<table>
<thead>
<tr>
<th>( a )</th>
<th>(1)</th>
<th>(1 + i)</th>
<th>(2)</th>
<th>(2 + i)</th>
<th>(2 - i)</th>
<th>(2 + 2i)</th>
<th>(2 - i)</th>
<th>(3)</th>
<th>(3 + i)</th>
<th>(3 - i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N(a) )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>( \chi(a) )</td>
<td>1</td>
<td>-4</td>
<td>16</td>
<td>-7 + 24i</td>
<td>-7 - 24i</td>
<td>-64</td>
<td>81</td>
<td>28 - 96i</td>
<td>28 - 96i</td>
<td></td>
</tr>
</tbody>
</table>

This gives the Dirichlet series

\[
L(\chi, s) = 1^{-s} - 4 \cdot 2^{-s} + 16 \cdot 4^{-s} - 14 \cdot 5^{-s} - 64 \cdot 8^{-s} + 81 \cdot 9^{-s} + 56 \cdot 10^{-s} + \cdots
\]

and the Euler product

\[
L(\chi, s) = \frac{1}{1 + 2^2 \cdot 2^{-s}} \cdot \frac{1}{1 - (-7 + 24i) \cdot 5^{-s}} \cdot \frac{1}{1 - (-7 - 24i) \cdot 5^{-s}} \cdot \frac{1}{1 - 9^2 \cdot 9^{-s}} \cdots
= \frac{1}{1 + 2^2 \cdot 2^{-s}} \cdot \frac{1}{1 - 3^4 \cdot 3^{-2s}} \cdot \frac{1}{1 - 14 \cdot 5^{-s} + 5^4 \cdot 5^{-2s}} \cdots.
\]

1.3 Modular forms and elliptic curves

1.3.1 Elliptic curves

Let \( E \) be an elliptic curve over \( \mathbb{Q} \), given by a Weierstrass equation

\[
E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6
\]

with coefficients \( a_1, \ldots, a_6 \in \mathbb{Z} \). We will assume that this equation has minimal discriminant among all Weierstrass equations for \( E \) with integral coefficients. For every prime power \( q = p^n \), we let \( \mathbb{F}_q \) denote a finite field with \( q \) elements, and we consider the number of points of \( E \) over \( \mathbb{F}_q \). Including the point at infinity, the number of points is

\[
\#E(\mathbb{F}_q) = 1 + \# \{(x, y) \in \mathbb{F}_q \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0 \}.
\]

For every prime number \( p \), we then define a power series \( \zeta_{E,p} \in \mathbb{Q}[[t]] \) by

\[
\zeta_{E,p} = \exp \left( \sum_{m=1}^{\infty} \frac{\#E(\mathbb{F}_{p^m})}{m} t^m \right).
\]
Theorem 1.10 (Schmidt, 1931; Hasse, 1934). If $E$ has good reduction at $p$, then there exists an integer $a_p$ such that

$$\zeta_{E,p} = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)} \in \mathbb{Z}[[t]].$$

Furthermore, $a_p$ satisfies

$$|a_p| \leq 2\sqrt{p}.$$

Looking at the coefficient of $t$ in $\zeta_{E,p}$, we see in particular that the number of $\mathbb{F}_p$-rational points is given in terms of $a_p$ by

$$\#E(\mathbb{F}_p) = p + 1 - a_p. \tag{1.3}$$

Next, suppose that $E$ has bad reduction at $p$. Then an analogue of Theorem 1.10 holds without the term $pt^2$, and the formula (1.3) remains valid. In this case, there are only three possibilities for $a_p$, namely

$$a_p = \begin{cases} 
1 & \text{if } E \text{ has split multiplicative reduction at } p, \\
-1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\
0 & \text{if } E \text{ has additive reduction at } p.
\end{cases}$$

Remark 1.11. If $E$ has bad reduction at $p$, then the reduction of $E$ modulo $p$ has a unique singular point, and this point is $\mathbb{F}_p$-rational. The formula (1.3) for $\#E(\mathbb{F}_p)$ includes this singular point. It is not obvious at first sight whether this point should be included in $\#E(\mathbb{F}_p)$ or not; it turns out that including it is the right choice for defining the $L$-function.

We combine all the functions $\zeta_{E,p}$ by putting

$$\zeta_E(s) = \prod_{p \text{ prime}} \zeta_{E,p}(p^{-s}).$$

By Theorem 1.10, the infinite product converges absolutely and uniformly on every set of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with $\sigma > 3/2$.

More generally, one can try to find out what happens when we replace the elliptic curve $E$ by a more general variety $X$ (more precisely, a scheme of finite type over $\mathbb{Z}$). We can define local factors $\zeta_{X,p}$ and their product

$$\zeta_X(s) = \prod_{p \text{ prime}} \zeta_{X,p}(p^{-s}).$$

in the same way as above; some care must be taken at primes of bad reduction. However, much less is known about the properties of $\zeta_X(s)$ for general $X$. The function $\zeta_X(s)$ is known as the Hasse–Weil $\zeta$-function of $X$, and the Hasse–Weil conjecture predicts that $\zeta_X(s)$ can be extended to a meromorphic function on the whole complex plane, satisfying a certain functional equation.

For elliptic curves $E$ over $\mathbb{Q}$, the Hasse–Weil conjecture is true because of the modularity theorem, which implies that $\zeta_E(s)$ can be expressed in terms of the Riemann $\zeta$-function and the $L$-function of a modular form. More generally, for other varieties $X$, one may try to express $\zeta_X(s)$ in terms of “modular”, or more appropriately, “automorphic” objects, and use these to establish the desired analytic properties of $\zeta_X(s)$. This is one of the motivations for the Langlands conjecture.
Remark 1.12. For an interesting overview of both the mathematics and the history behind \( \zeta \)-functions and the problem of counting points on varieties over finite fields, see F. Oort’s article [6].

1.3.2 Modular forms
We will denote by \( \mathcal{H} \) the upper half-plane
\[
\mathcal{H} = \{ z \in \mathbb{C} | \Im z > 0 \}.
\]
This is a one-dimensional complex manifold equipped with a continuous left action of the group
\[
\text{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}.
\]
A particular role will be played by the group
\[
\text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}
\]
and the groups
\[
\Gamma(n) = \left\{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod n \right\}
\]
for \( n \geq 1 \).

Definition 1.13. A congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \) is a subgroup of \( \text{SL}_2(\mathbb{Z}) \) that contains \( \Gamma(n) \) for some \( n \geq 1 \).

Definition 1.14. Let \( \Gamma \) be a congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \), and let \( k \) be a positive integer. A modular form of weight \( k \) is a holomorphic function
\[
f : \mathcal{H} \rightarrow \mathbb{C}
\]
with the following properties:

(i) For all \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \), we have
\[
f \left( \frac{az + b}{cz + d} \right) = (cz + d)^k f(z).
\]

(ii) The function \( f \) is “holomorphic at the cusps of \( \Gamma \)”. (We will not make this precise now.)

From now on we assume (for simplicity) that \( \Gamma \) is of the form
\[
\Gamma_1(n) = \left\{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod n \right\}
\]
for some \( n \geq 1 \). Then \( \Gamma \) contains the matrix \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). Then the above definition implies that every modular form for \( \Gamma \) can be written as
\[
f(z) = \sum_{m=0}^{\infty} a_m \exp(2\pi i z) \quad \text{with } a_0, a_1, \ldots \in \mathbb{C}.
\]
1.4 More examples of $L$-functions

1.4.1 Artin $L$-functions

We now introduce Artin $L$-functions, which are among the most fundamental examples of $L$-functions in the “arithmetic world”. The easiest non-trivial Artin $L$-functions are already implicit in the quadratic reciprocity law, and are obtained as follows.

Example 1.15. Let $K$ be a quadratic field of discriminant $d$, so that $K = \mathbb{Q}(\sqrt{d})$. Furthermore, let $\epsilon_K$ be the unique isomorphism $\text{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}$. Similarly to what we did in §1.1, to every prime $p$ that is unramified in $K$ (i.e. to every prime $p \nmid d$), we associate a Frobenius element $\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})$ by putting

$$\text{Frob}_p = \begin{cases} 
\text{id} & \text{if } p \text{ splits in } K, \\
\sigma & \text{if } p \text{ is inert in } K.
\end{cases}$$

In other words, we have

$$\text{Frob}_p = \left(\frac{d}{p}\right)$$

The Artin $L$-function attached to $\epsilon_K$ is then defined by the Euler product

$$L(\epsilon_K, s) = \prod_{p \text{ unramified in } K} (1 - \epsilon_K(\text{Frob}_p)p^{-s})^{-1} = \prod_{p \text{ prime}} \left(1 - \left(\frac{d}{p}\right)p^{-s}\right)^{-1}.$$  

The quadratic reciprocity law can be viewed as saying that if $q$ is a prime number and $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{(q-1)/2}q$, and $\chi_q$ is the quadratic Dirichlet character defined by $\chi_q(a \text{ mod } q) = \left(\frac{a}{q}\right)$, then we have an equality of $L$-functions

$$L(\epsilon_K, s) = L(\chi_q, s).$$

As a first step towards studying non-Abelian Galois groups and their (higher-dimensional) representations, we make the following definition.

Definition 1.16. Let $K$ be a finite Galois extension of $\mathbb{Q}$, and let $n$ be a positive integer. An Artin representation is a group homomorphism

$$\rho: \text{Gal}(K/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{C}).$$

Artin representations are examples of Galois representations. More general Galois representations are obtained by looking at arbitrary Galois extensions of fields and $\text{GL}_n$ over other rings.

Remark 1.17. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and view $K$ as a subfield of $\overline{\mathbb{Q}}$ by choosing an embedding. Then $\text{Gal}(K/\mathbb{Q})$ is a finite quotient of the infinite Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Just as we can view a Dirichlet character as a continuous one-dimensional $\mathbb{C}$-linear representation of the topological group $\mathbb{Z}^\times$, we can view an Artin representation as a continuous $n$-dimensional $\mathbb{C}$-linear representation of the topological group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ factoring through the quotient map $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q})$. 

Next, we want to attach an $L$-function to an Artin representation. If $p$ is a prime number such that the number field $K$ is unramified at $p$, then we can define a Frobenius conjugacy class at $p$ in $\text{Gal}(K/\mathbb{Q})$. If $\sigma_p$ is any Frobenius element at $p$ (i.e. an element of the Frobenius conjugacy class), then we define the characteristic polynomial of Frobenius $F_{\rho,p} \in \mathbb{C}[t]$ by the formula

$$F_{\rho,p} = \det(1 - \rho(\sigma_p)t) \in \mathbb{C}[t].$$

(This is the determinant of an $n \times n$-matrix with coefficients in $\mathbb{C}[t]$.) More generally, if $K$ is possibly ramified at $p$, we have to modify the above definition; this gives rise to a polynomial $F_{\rho,p} \in \mathbb{C}[t]$ of degree at most $n$.

**Definition 1.18.** Let $\rho: \text{Gal}(K/\mathbb{Q}) \to \text{GL}_n(\mathbb{C})$ be an Artin representation. The Artin $L$-function of $\rho$ is the function

$$\prod_{p \text{ prime}} \frac{1}{F_{\rho,p}(p^{-s})}.$$ 

One can show that the product converges absolutely and uniformly for $s$ in sets of the form $\{s \in \mathbb{C} \mid \Re s \geq a\}$ with $a \geq 1$.

**Example 1.19.** Let $K$ be the splitting field of the irreducible polynomial $f = x^3 - x - 1 \in \mathbb{Q}[x]$. Because the discriminant of $f$ equals $-23$, which is not a square, we have

$$K = \mathbb{Q}(\alpha, \sqrt{-23}),$$

where $\alpha$ is a solution of $\alpha^3 - \alpha - 1 = 0$. The number field $K$ has discriminant $-23^3$, and the Galois group of $K$ over $\mathbb{Q}$ is isomorphic to the symmetric group $S_3$ of order 6.

The group $S_3$ has a two-dimensional representation $S_3 \to \text{GL}_2(\mathbb{C})$ defined by

$$(1) \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (12) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad (13) \mapsto \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

$$(23) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (132) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$ 

Composing this with some isomorphism $\text{Gal}(K/\mathbb{Q}) \overset{\sim}{\to} S_3$ gives an Artin representation

$$\rho: \text{Gal}(K/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}).$$

The Frobenius conjugacy class at a prime $p$ can be read off from the splitting behaviour of $p$ in $K$, which in turn can be read off from the number of roots of the polynomial $x^3 - x - 1$ modulo $p$. (These are only equivalent because the Galois group is so small; for general Galois groups, the situation is more complicated.) It is a small exercise to show that for a prime number $p \neq 23$, there are three possibilities:

- $-23$ is a square modulo $p$, the polynomial $x^3 - x - 1$ has three roots modulo $p$, and the Frobenius conjugacy class is $\{(1)\}$;

- $-23$ is a square modulo $p$, the polynomial $x^3 - x - 1$ has no roots modulo $p$, and the Frobenius conjugacy class is $\{(123), (132)\}$;

- $-23$ is not a square modulo $p$, the polynomial $x^3 - x - 1$ has exactly one root modulo $p$, and the Frobenius conjugacy class is $\{(12), (13), (23)\}$. 
Moreover, one computes the polynomial \( F_{\rho,p} \in \mathbb{C}[t] \) by taking the characteristic polynomial of the matrices in the corresponding Frobenius conjugacy class. For the first few prime numbers \( p \), this gives

\[
\begin{array}{c|cccccccc}
p & 2 & 3 & 5 & 7 & 11 & 23 & 59 & \\
\sigma_p [\rho,p] & (123) & (123) & (12) & (12) & - & (1) & \\
F_{\rho,p} & 1 + t + t^2 & 1 + t + t^2 & 1 - t^2 & 1 - t^2 & 1 - t & \\
\end{array}
\]

The Euler product and Dirichlet series of \( L(\rho,s) \) look like

\[
L(\rho,s) = \frac{1}{1 + 2^{-s} + 2^{-2s}} \cdot \frac{1}{1 + 3^{-s} + 3^{-2s}} \cdot \frac{1}{1 - 5^{-2s}} \cdot \frac{1}{1 - 7^{-2s}} \cdots
\]

\[
= 1^{\sigma} - 2^{-s} - 3^{-s} + 6^{-s} + 8^{-s} - 13^{-s} - 16^{-s} + 23^{-s} - 24^{-s} + \cdots.
\]

1.4.2 \( L \)-functions attached to elliptic curves

We have seen several examples of \( L \)-functions attached to number-theoretic objects such as number fields, Dirichlet characters and Artin representations. It turns out to be very fruitful to define \( L \)-functions for geometric objects as well. Our first example is that of elliptic curves over \( \mathbb{Q} \).

Let \( E \) be an elliptic curve over \( \mathbb{Q} \). For every prime number \( p \), we define \( a_p \) as in §1.3.1, and we put

\[
\epsilon(p) = \begin{cases} 1 & \text{if } E \text{ has good reduction at } p, \\ 0 & \text{if } E \text{ has bad reduction at } p. \end{cases}
\]

We can now define the \( L \)-function of the elliptic curve \( E \) as

\[
L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}}.
\]

As we saw in §1.3.1, this infinite product defines a holomorphic function \( L(E,s) \) on the right half-plane \( \{ s \in \mathbb{C} \mid \Re s > 3/2 \} \). Furthermore, the \( \zeta \)-function of \( E \) can be expressed as

\[
\zeta_E(s) = \frac{\zeta(s) \zeta(s-1)}{L(E,s)}.
\]

Example 1.20. Let \( E \) be the elliptic curve

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

This curve has bad reduction at the primes 2 and 3. Counting points on \( E \) over the fields \( \mathbb{F}_p \) for \( p \in \{2, 3, 5, 7, 11\} \) gives

\[
\begin{array}{c|cccc}
p & 2 & 3 & 5 & 7 & 11 \\
a_p & 0 & -1 & -2 & 0 & 4 \\
\end{array}
\]

This shows that the \( L \)-function of \( E \) looks like

\[
L(E,s) = \frac{1}{1} \cdot \frac{1}{1 + 3^{-s}} \cdot \frac{1}{1 + 2 \cdot 5^{-s} + 5^{-2s}} \cdot \frac{1}{1 + 7 \cdot 7^{-2s}} \cdot \frac{1}{1 - 4 \cdot 11^{-s} + 11 \cdot 11^{-2s}} \cdots
\]

\[
= 1^{-s} - 3^{-s} - 2 \cdot 5^{-s} + 9^{-s} + 4 \cdot 11^{-s} + \cdots
\]
We recall that by the Mordell–Weil theorem, the set $E(\mathbb{Q})$ of rational points on $E$ has the structure of a finitely generated Abelian group. The rank of this Abelian group is still far from understood; it is expected to be linked to the $L$-function of $E$ by the following famous conjecture.

**Conjecture 1.21** (Birch and Swinnerton-Dyer). Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $L(E, s)$ can be continued to a holomorphic function on the whole complex plane, and its order of vanishing at $s = 1$ equals the rank of $E(\mathbb{Q})$.

Some partial results on this conjecture are known; in particular, it follows from work of Gross, Zagier and Kolyvagin that if the order of vanishing of $L(E, s)$ at $s = 1$ is at most 1, then this order of vanishing is equal to the rank of $E(\mathbb{Q})$.

**Remark 1.22.** There exists a refined version of the conjecture of Birch and Swinnerton-Dyer that also predicts the leading term in the power series expansion of $L(E, s)$ around $s = 1$. The predicted value involves various arithmetic invariants of $E$; explaining these is beyond the scope of this course.

### 1.4.3 $L$-functions attached to modular forms

Let $n$ and $k$ be positive integers, and let $f$ be a modular form of weight $k$ for the group $\Gamma_1(n)$, with $q$-expansion

$$f(z) = \sum_{m=0}^{\infty} a_m q^m \quad (q = \exp(2\pi i z)).$$

The $L$-function of $f$ is defined as the Dirichlet series

$$L(f, s) = \sum_{m=1}^{\infty} a_m m^{-s}$$

for $\Re s > (k+1)/2$. (Note that $a_0$ does not appear in the sum defining $L(f, s)$.)

Furthermore, we define the completed $L$-function attached to $f$ as

$$\Lambda(f, s) = n^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(f, s).$$

**Theorem 1.23.** Suppose $f$ is a primitive cusp form. Then $\Lambda(f, s)$ can be continued to a holomorphic function on all of $\mathbb{C}$. Furthermore, there exist a primitive cusp form $f^*$ and a complex number $\epsilon_f$ of absolute value 1 such that $\Lambda(f, s)$ and $\Lambda(f^*, s)$ are related by the functional equation

$$\Lambda(f, k-s) = \epsilon_f \Lambda(f^*, s).$$

The proof of this theorem has some similarities to that of Theorem 1.2. The main tools are the theory of newforms, the Fricke (or Atkin–Lehner) operator $w_n$, and the Mellin transform.

The following theorem was proved by Wiles in 1993, with an important contribution by Taylor, in the case of semi-stable elliptic curves, i.e. curves having good or multiplicative reduction at every prime. The proof for general elliptic curves was finished by a sequence of papers by Breuil, Conrad, Diamond and Taylor.
Theorem 1.24 (Modularity of elliptic curves over \( \mathbb{Q} \)). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then there exist a positive integer \( n \) and a primitive cusp form \( f \) of weight 2 for the group \( \Gamma_0(n) \) such that
\[
L(E, s) = L(f, s).
\]

1.5 Exercises

Exercise 1.1. Let \( p \) be an odd prime number. Prove the following formulae for the Legendre symbol \( (\frac{-1}{p}) \):
\[
(\frac{-1}{p}) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}; 
\end{cases}
\]
\[
(\frac{2}{p}) = \begin{cases} 
1 & \text{if } p \equiv 1,7 \pmod{8}, \\
-1 & \text{if } p \equiv 3,5 \pmod{8}; 
\end{cases}
\]
\[
(\frac{-2}{p}) = \begin{cases} 
1 & \text{if } p \equiv 1,3 \pmod{8}, \\
-1 & \text{if } p \equiv 5,7 \pmod{8}. 
\end{cases}
\]

(Hint: embed the quadratic fields \( \mathbb{Q}(\sqrt{d}) \) for \( d \in \{-1, 2, -2\} \) into the cyclotomic field \( \mathbb{Q}(\zeta_8) \).)

Remark: Together with the quadratic reciprocity law \( (\frac{q}{p}) = (-1)^{(p-1)(q-1)/2} (\frac{q}{p}) \) for odd prime numbers \( q \neq p \), these formulae make it possible to express \( (\frac{a}{p}) \) in terms of congruence conditions on \( p \) for all \( a \in \mathbb{Z} \).

Exercise 1.2. Let \( K \) be a quadratic field, and let \( \epsilon_K \) be the unique injective homomorphism from \( \text{Gal}(K/\mathbb{Q}) \) to \( \mathbb{C}^\times \). Prove the identity
\[
\zeta_K(s) = \zeta(s)L(\epsilon_K, s).
\]

Exercise 1.3. Show that the character \( \chi : I \to \mathbb{C}^\times \) defined in §1.2.4, where \( I \) the group of fractional ideals of \( \mathbb{Z}[\sqrt{-1}] \), is injective.

Exercise 1.4. Let \( \chi \) be a Dirichlet character modulo \( n \). We consider the function \( \mathbb{Z} \to \mathbb{C} \) sending an integer \( m \) to the complex number
\[
\tau(\chi, m) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi i jm/n).
\]
(This can be viewed as a discrete Fourier transform of \( \chi \).) The case \( m = 1 \) deserves special mention: the complex number
\[
\tau(\chi) = \tau(\chi, 1) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi i j/n)
\]
is called the Gauss sum attached to \( \chi \).

(a) Compute \( \tau(\chi) \) for all non-trivial Dirichlet characters \( \chi \) modulo 4 and modulo 5, respectively.
(b) Suppose that $\chi$ is primitive. Prove that for all $m \in \mathbb{Z}$ we have
\[ \tau(\chi, m) = \bar{\chi}(m)\tau(\chi). \]

(Hint: writing $d = \gcd(m, n)$, distinguish the cases $d = 1$ and $d > 1$.)

(c) Deduce that if $\chi$ is primitive, we have
\[ \tau(\chi)\tau(\bar{\chi}) = \chi(-1)n \]
and
\[ \tau(\chi)\tau(\bar{\chi}) = n. \]

**Exercise 1.5.** Let $\chi$ be a primitive Dirichlet character modulo $n$. The **generalised Bernoulli numbers** attached to $\chi$ are the complex numbers $B_k(\chi)$ for $k \geq 0$ defined by the identity
\[ \sum_{k=0}^{\infty} \frac{B_k(\chi)}{k!} t^k = \frac{t}{\exp(nt) - 1} \sum_{j=1}^{n} \chi(j) \exp(jt) \]
in the ring $\mathbb{C}[[t]]$ of formal power series in $t$.

(a) Prove that if $\chi$ is non-trivial (i.e. $n > 1$), then we have
\[ \sum_{j=0}^{n-1} \chi(j) \frac{x + \exp(2\pi i j/n)}{x - \exp(2\pi i j/n)} = \frac{2n}{\tau(\chi)(x^n - 1)} \sum_{m=0}^{n-1} \bar{\chi}(m)x^n \]
in the field $\mathbb{C}(x)$ of rational functions in the variable $x$. (Hint: compute residues.)

(b) Prove that for every integer $k \geq 2$ such that $(-1)^k = \chi(-1)$, the special value of the Dirichlet $L$-function of $\chi$ at $k$ is
\[ L(\chi, k) = -\frac{(2\pi i)^kB_k(\chi)}{2\tau(\chi)n^{k-1}k!}. \]

(Hint: use the identity $\frac{\cos z}{\sin z} = \frac{1}{z} + \sum_{m=1}^{\infty} \left( \frac{1}{z - m\pi} + \frac{1}{z + m\pi} \right)$.)

**Exercise 1.6.** Let $q$ be an odd prime number, and let $q^* = (-1)^{(q-1)/2}q$. Use Gauss sums to prove that there exists an inclusion of fields
\[ \mathbb{Q}(\sqrt{q^*}) \hookrightarrow \mathbb{Q}(\zeta_q). \]

**Exercise 1.7.** The **Fourier transform** of a quickly decreasing function $f : \mathbb{R} \to \mathbb{C}$ is defined by
\[ \hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi ixy)dx. \]

(a) Let $f : \mathbb{R} \to \mathbb{C}$ be a quickly decreasing function, let $c \in \mathbb{R}$, and let $f_c(x) = f(x + c)$. Show that $\hat{f}_c(y) = \exp(2\pi iyc)\hat{f}(y)$.

(b) Let $f : \mathbb{R} \to \mathbb{C}$ be a quickly decreasing function, let $c > 0$, and let $f_c(x) = f(cx)$. Show that $\hat{f}_c(y) = c^{-1}\hat{f}(y/c)$.
(c) Let \( g_+(x) = \exp(-\pi x^2) \). Show that \( \hat{g}_+(y) = g_+(y) \).

(d) Let \( g_-(x) = \pi x \exp(-\pi x^2) \). Show that \( \hat{g}_-(y) = -ig_-(y) \).

(Hint for (c) and (d): shift the line of integration in the complex plane.)

**Exercise 1.8.** Let \( n \) be a positive integer, and let \( \chi \) be a primitive Dirichlet character modulo \( n \). Recall that the Dirichlet \( L \)-function attached to \( \chi \) is defined by

\[
L(\chi, s) = \sum_{m=1}^{\infty} \chi(m) m^{-s} \quad \text{for } \Re s > 1.
\]

Recall that \( \chi \) is called *even* if \( \chi(-1) = 1 \) and *odd* if \( \chi(-1) = -1 \). We define the *completed Dirichlet \( L \)-function* \( \Lambda(\chi, s) \) by

\[
\Lambda(\chi, s) = \begin{cases} 
\frac{n^{s/2} \Gamma(s/2)}{\pi^{s/2}} L(\chi, s) & \text{if } \chi \text{ is even} \\
\frac{n^{s/2} \Gamma((s+1)/2)}{\pi^{(s-1)/2}} L(\chi, s) & \text{if } \chi \text{ is odd}
\end{cases}
\]

The goal of this exercise is to generalise the proof of Theorem 1.2 to show that \( \Lambda(\chi, s) \) admits an analytic continuation and functional equation.

We define two functions \( g_+, g_- : \mathbb{R} \to \mathbb{C} \) by

\[
g_+(x) = \exp(-\pi x^2), \quad g_-(x) = \pi x \exp(-\pi x^2).
\]

For every primitive Dirichlet character \( \chi \) modulo \( n \), we define a function

\[
\phi_\chi(t) = \begin{cases} 
\sum_{m \in \mathbb{Z}} \chi(m) g_+(mt) & \text{if } \chi \text{ is even,} \\
\sum_{m \in \mathbb{Z}} \chi(m) g_-(mt) & \text{if } \chi \text{ is odd.}
\end{cases}
\]

(a) Prove the identity

\[
\phi_\chi(t) = \begin{cases} 
\frac{\tau(\chi)}{nt} \phi_\chi(\frac{1}{nt}) & \text{if } \chi \text{ is even,} \\
\frac{\tau(\chi)}{nt} \phi_\chi(\frac{1}{nt}) & \text{if } \chi \text{ is odd.}
\end{cases}
\]

(Hint: use the Poisson summation formula and Exercises 1.4 and 1.7)

From now on, we assume that \( \chi \) is non-trivial, i.e. \( n > 1 \).

(b) Give asymptotic expressions for \( \phi_\chi(t) \) as \( t \to 0 \) and as \( t \to \infty \). (Note: the answer depends on \( \chi \).)

(c) Let \( \mathcal{M}\phi_\chi \) be the Mellin transform of \( \phi_\chi \), defined by

\[
(M\phi_\chi)(s) = \int_0^\infty \phi_\chi(t) t^{s-1} dt.
\]

Prove that the integral converges for all \( s \in \mathbb{C} \), and that the completed \( L \)-function can be expressed as

\[
\Lambda(\chi, s) = n^{s/2}(M\phi_\chi)(s) \quad \text{for } \Re s > 1.
\]
(d) Conclude that $\Lambda(\chi, s)$ can be continued to a holomorphic function on all of $\mathbb{C}$ (without poles), and that $\Lambda(\chi, s)$ and $\Lambda(\bar{\chi}, s)$ are related by the functional equation

$$\Lambda(\chi, s) = \epsilon_\chi \Lambda(\bar{\chi}, 1 - s),$$

where $\epsilon_\chi$ is the complex number of absolute value 1 defined by

$$\epsilon_\chi = \begin{cases} \frac{\tau(\chi)}{\sqrt{n}} & \text{if } \chi \text{ is even,} \\ \frac{\tau(\chi)}{i\sqrt{n}} & \text{if } \chi \text{ is odd.} \end{cases}$$

**Exercise 1.9.** Let $a, b \in \mathbb{Z}$, and suppose that the integer $\Delta = -16(4a^3 + 27b^2)$ is non-zero. Let $E$ over $\mathbb{Z}[1/\Delta]$ be the elliptic curve given by the equation $y^2 = x^3 + ax + b$. Let $p$ be a prime number not dividing $\Delta$, and write

$$N_E(\mathbb{F}_p) = 1 + \#\{(x, y) \in \mathbb{F}_p \mid y^2 = x^3 + ax + b\}.$$ 

Prove that

$$N_E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left( \left( \frac{x^3 + ax + b}{p} \right) + 1 \right),$$

where $(\cdot)$ is the Legendre symbol.

**Exercise 1.10.** Up to isogeny, there are three distinct elliptic curves of conductor 57, namely

- $E_1: y^2 + y = x^3 - x^2 - 2x + 2,$
- $E_2: y^2 + xy + y = x^3 - 2x - 1,$
- $E_3: y^2 + y = x^3 + x^2 + 20x - 32.$

The newforms of weight 2 for the group $\Gamma_0(57)$ are

- $f_1 = q - 2q^2 - q^3 + 2q^4 - 3q^5 + O(q^6),$
- $f_2 = q - 2q^2 + q^3 + 2q^4 + q^5 + O(q^6),$
- $f_3 = q + q^2 + q^3 - q^4 - 2q^5 + O(q^6).$

Which form corresponds to which elliptic curve under Wiles’s modularity theorem?
Bibliography


