S*pringer* **M***onographs in* **M***athematics*

For further volumes:
http://www.springer.com/series/3733

Haruzo Hida

Elliptic Curves and Arithmetic Invariants

Springer

Haruzo Hida
Department of Mathematics
University of California
Los Angeles, CA, USA

ISSN 1439-7382
ISBN 978-1-4614-6656-7 ISBN 978-1-4614-6657-4 (eBook)
DOI 10.1007/978-1-4614-6657-4
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013937713

Mathematics Subject Classification: 11F11, 11F25, 11G18, 11G15, 11F80, 11R23, 11F67, 11G05, 11F80

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Number theorists study arithmetic objects by attaching invariants to them to make them clearly visible. Each important research object in number theory has its L-functions. As they are functions of complex or p-adic variables, we can evaluate them at integers, getting concrete numbers from the starting object.

The Archimedean L-function (in this book) has a functional equation. If the value of its Γ-factor and its counterpart under the functional equation neither vanish nor have a pole at an integer m, assuming that the L-function at m is finite, we call such an m critical with respect to the L-function. If m is critical for the L-function, the value is expected to give an algebraic number up to a canonical transcendental factor (called a period, which often behaves compatibly under algebraic operations, for example, direct product of the objects, tensor product, and so on). Such phenomena were first found by Euler in the mid-18th century for the Riemann zeta function and were rediscovered in the 1970s by Shimura for many automorphic/geometric L-functions. Today we benefit from a good analysis both of the automorphic period of automorphic L-values through the work of Shimura and others as well as that of the geometric period of algebraic varieties and motives from the work of Shimura, Deligne, and others.

Here arises a typical number-theoretic question comparing the automorphic/geometric definitions of a period: Once an automorphic form is attached to a geometric object, such as an abelian variety or, more generally, a motive, do the automorphic period and the geometric period coincide? Assuming holomorphy of the L-function and the Γ-factor at an evaluating integer s_0, if s_0 is not critical, the Γ-factor has a pole at the reflex point s_0' of s_0, and the L-value at s_0' would simply be 0. Thus, its derivative at s_0' is related by the functional equation to the value at the original point s_0 up to a correction factor in addition to the period. The correction factor is an interesting new invariant, the *regulator*, which depends crucially both on the arithmetic object and on the point of evaluation.

Once the algebraic part of critical L-values is well defined, we might want to relate it to a new arithmetic object produced from the starting object. For example, if we are given an imaginary quadratic field, from its reciprocity law we can produce a Dirichlet L-function whose value at the critical point 0 is essentially the order of the class group of the imaginary quadratic field (Dirichlet's celebrated class number formula). Dirichlet's formula is the identity between two arithmetic invariants: One is given by the value at 0 of the L-function associated with the imaginary quadratic field, and the other is the order of a finite abelian group specifically produced out of the integer ring of the field.

Going further, we might want to search a p-adic analytic L-function having the same value (up to a simple *p-adic modification factor* similar to an Euler factor) at critical evaluation points. Again, we therefore get a p-adic period and a p-adic regulator and an arithmetic object (now somehow p-adically made) whose size is (often conjecturally) given by the value or the derivative (possibly up to the p-adic regulator).

The p-adic modification factor rarely (but sometimes) vanishes at some integer points (producing an exceptional zero of the p-adic L-function), making the p-adic critical value close to an Archimedean noncritical value. The p-adic derivative of the p-adic L-function is equal up to a factor $\mathcal{L}$, similar to the regulator, to the (algebraic part of) Archimedean L-value, getting another invariant, called the $\mathcal{L}$-invariant. Mazur–Tate–Teitelbaum systematically studied the $\mathcal{L}$ although the value of the $\mathcal{L}$ was studied and even determined for some specific L-functions earlier than their work.

One may look into the growth of L-values over points densely populated in the domain of the L-function. Suppose that a p-adic L-function L_p is defined on a unit disk of p-adic numbers. If its p-adic absolute values $|L_p(s)|_p$ are bounded by the supremum $p^{-\mu}$ for $0 \leq \mu \in \mathbb{Q}$, this μ is the μ-invariant first studied by Iwasawa in the 1960s and 1970s. Iwasawa then defined his λ-invariant to be the number of zeros of the p-adic L-function (counted with multiplicity) in order to measure the growth of a p-adic Dirichlet L-function and the growth of the p-part of the class numbers of the cyclotomic fields of p-power roots of unity.

If we are given a compatible system of l-adic Galois representations, its trace a_p of the p-Frobenius element at unramified primes p outside l is algebraic and independent of l. This a_p itself is an invariant describing the structure of the Galois group (and also the local Galois group at p) of the splitting Galois extension of the representation, and we may uniquely form an Archimedean L-function $\sum_{n=1}^{\infty} c_n n^{-s}$ with Euler product converging for $\mathrm{Re}(s) \gg 0$ having $c_p = a_p$ for primes p from it. Or we can study the field generated by a_p over the rational numbers $\mathbb{Q}$, which is called the Hecke field of the system if the system comes from an automorphic/modular form (as we expect that every system comes from an appropriately chosen automorphic

form). Once a Hecke field is given, its degree over the rational numbers is a most primitive example of the invariants attached to the system.

Often the definition of the invariant itself does not give us a straight way of understanding it. So number theorists seek a more direct or theoretical way to compute the invariant. This is done in many cases through heuristic understandings of the invariant. For example, the critical/noncritical L-value is supposed to compute the order of an arithmetically defined abelian group (an arithmetic cohomology group, called a Selmer group) similarly to the Dirichlet class number formula. If we could prove this heuristic, it would be a generalization of Dirichlet's class number formula. Some mathematicians have tried to specify what kind of arithmetic cohomology group should appear this way (i.e., the Bloch–Kato conjecture for general motives; more specifically, the Birch–Swinnerton-Dyer conjecture if the L-function is associated with a rational elliptic curve and the evaluation point of interest is $s = 1$). This is an identification problem of two different invariants, one analytically defined and the other arithmetically defined. Similarly, Shimura and Deligne have studied the equality of the automorphic period and the geometric period. All of these problems (which are central to present-day number theory) can be summarized into a set of problems targeting an identity of two or more different definitions/incarnations of the invariant.

Since miraculous (and possibly profound) formulas are scattered throughout number theory, mathematicians working in this area tend to seek a new one directly or indirectly relating different arithmetic invariants. Most of the celebrated conjectures in this research area fall into this category out of the desire to convince ourselves of the harmony of our universe. I am not at all against the idea. However, before setting out to see the God-given harmony of numbers, we would do better to worry about the nontriviality or triviality of the invariant. For example, Ferrero–Washington proved the vanishing of the (original) Iwasawa μ-invariant long ago in an elementary way. The vanishing is equivalent to the nontriviality of the p-adic L-function modulo p. From their result, if Iwasawa's λ-invariant vanishes (i.e., is trivial) very often, we get the infinity of regular primes (does the name indicate that regular primes must be "regularly" found?). This type of banal outcome, though possibly deep, is often more intriguing in its proof than in the proof of a nice formula connecting far-reaching arithmetic objects. Furthermore, as the outcome is banal, one may not be able to develop a conjectural formula from the problem (which satisfies mathematicians' aesthetic desires).

The critical L-values must be generically nonzero (with interesting and rare exceptions) unless the vanishing is forced by some trivial reason, and its first derivatives must be nonzero most of the time if the vanishing is forced. This is basically telling us that normally we are working in an easy environment (without the need to worry about the triviality of the invariant). We should be working in "regular" cases (of nonvanishing L-values) to produce the formulas in most instances, rather than working against hostility, requiring

heroic efforts to prove an identity of higher derivatives. The regulators must not vanish in most of the cases (nonvanishing is often assumed by the lack of its proof), but to my knowledge, nobody seems to have made a systematic algebraic/arithmetic theory aimed at showing the nontriviality/triviality of the invariant.

In summary, there appear to be two fundamental problems concerning the invariants in number theory:

A. Find (even conjecturally) a relation (or an identity) of two or more arithmetic invariants of a different nature.
B. Prove the nontriviality/triviality of important arithmetic invariants.

In the early 1990s, I somehow realized the importance of problem B (and of making an algebraic theory dealing with it) and started working on it, although I still continue to work out things belonging to problem A. A principle (useful in attacking problem B) I came up with is rather ordinary:

If we want to show algebraically the nonvanishing of some value, in practice, the only way is to spread or interpolate the values as a good function over a geometric object (say, an algebraic variety that parameterizes the different values we study). If we could show that the function is nonconstant, there are not many zeros; hence, its specialization to the value we want is often nonzero. If we are able to go farther, we can even show that the zero set of the function somehow avoids all specific points of our interest (thus, getting the nontriviality of "each" desired value).

This book is the first report on my effort for the past 20 years, and I hope to present my progress report covering more new topics in the near future (as I believe that the method should be amenable to generalizations and has much room for improvement, because of the simplicity of the idea). We limit ourselves to topics directly related to elliptic modular forms (to make this book accessible to graduate students), though many results can be generalized (at least) to Hilbert modular forms (such generalizations are often given in my research articles quoted in the text).

Here is an outline of the book. In Chap. 1, after giving definitions of Iwasawa's invariants and the $\mathcal{L}$-invariants, as an example of the above principle, we reproduce Sinnott's proof of the nonvanishing of Dirichlet L-values modulo p (originally proven by L. Washington in 1978) under twists by most characters modulo l-power for a prime $l \neq p$. Then we go on to describe an outline of the proof of the rationality of Hecke L-values by Shimura and its p-adic version by Katz; hence, we get p-adic Hecke L-functions (of imaginary quadratic fields). For rationality, we need the invariant differential operators acting either on C^∞ modular forms or on p-adic modular forms. Shimura prominently resurrected the use of such operators (going back to Maass) to prove the rationality results of modular/automorphic L-values up to "periods," and Katz made its p-adic "avatar." We will give perhaps the simplest

construction (which I found about 20 years ago) of the p-adic operator, which connects directly with Archimedean operators and which requires only the deformation theory of ordinary elliptic curves as a tool (and should be easily generalized to the ordinary locus of Shimura varieties of PEL type).

In Chap. 2, without becoming too technical, we recall the geometric definition of elliptic modular forms (and moduli problems of elliptic curves over fields) just for our use in Chap. 3 to state the main results.

Almost all the main themes of the book appear in Chap. 3, possibly without a detailed proof. We prove the fast growth of the degree of Hecke fields for non-CM analytic families of slope 0, the nonvanishing (in most cases) of the $\mathcal{L}$-invariant of the modular adjoint L-function at $s = 1$ (restricting ourselves to simplest cases), and a sketch of a proof of the vanishing of the μ-invariant of Katz p-adic L-functions. At the end, we state a principle of distinguishing mod-p Shimura subvarieties of a Shimura variety as a subvariety stable under Hecke correspondences (Chai–Oort's rigidity principle, an example of problem A), which is heavily used in the proof of the vanishing of the μ-invariant. This includes a brief outline of the theory of modular curves as a Shimura variety (and the Igusa tower over it).

Chapter 4 is an introduction to functorial scheme theory (and tools we need for fully proving some results illustrated in Chap. 3). Proofs of some theorems are given in a different way from other books for algebraic geometers (which is often unilluminating for number theorists). Some ring-theoretic results and more geometric results are quoted from different sources. Chapter 5 is a continuation of Chap. 4 but gathers more classical geometric results for varieties over a field. Readers who are familiar with functorial algebraic geometry or who just want to know the results for problem B without going into technicalities may skip these two chapters.

Chapter 6 is a detailed description of modular curves of individual levels over general rings. In particular, it contains a detailed description of deformation coordinates of the modular curve around an ordinary elliptic curve with complex multiplication. The study of the move of the deformation coordinate under the natural action of the stabilizer of the origin of the deformation space (carrying the CM elliptic curve) is a main tool to prove the rigidity principle.

In Chap. 7, we interpret the theory given in Chap. 6 in Shimura's way as the simplest of Shimura varieties. In addition, we complete and legitimize the sketchy construction of p-adic invariant differential operators first given in Chap. 1 (in Sect. 7.2.6). We also prove the irreducibility of the Igusa tower in the way given in [PAF] in more down-to-earth terms (which is the basis of the q-expansion principle essential in computing μ-invariants).

In Chap. 8, we generalize Sinnott's method (reproduced in Chap. 1) of proving the nonvanishing modulo p of Dirichlet L-values to Hecke L-values via the theory of Shimura varieties.

Chapter 9 is devoted to the proof of the vanishing of the μ-invariant of the p-adic Hecke L-functions (of each imaginary quadratic field) via a detailed analysis of the q-expansion of Eisenstein series. The rigidity principle and the

q-expansion principle (based on the irreducibility of the Igusa tower) play a prominent role.

In Chap. 10, we give a proof of Chai's local rigidity lemmas that is essential to prove the rigidity principle. In the last chapter, Chap. 11, we prove the rigidity principle for the elliptic Shimura curve and products of the copies of the curve (making this book logically complete).

This book's target audience encompasses graduate students (who already know the basics of elliptic modular forms, for example, as described in Chaps. 1–5 of [IAT]), postdoctoral scholars, and senior researchers working in the field of number theory.

In 2011, my graduate students Bin Zhao and Ashay Burungale (respectively in their third and second year of graduate school at UCLA) read most of the manuscript and suggested many improvements. I personally thank them for their careful reading.

In the hope of giving a good introductory account of my earlier (but more difficult) book [PAF], I started writing the manuscript while I was visiting l'Institut Henri Poincaré (Paris, France) in January–March of 2010 and continued writing while I visited Kyoto University in Japan from September to December 2010, partially supported by Clay Mathematics Institute as a senior scholar. I gave many lectures on the topics of this book at these institutions. I thank the audiences of my lectures for their enthusiasm/criticism and also thank these institutions for their hospitality and support. I hope that the original purpose of an introductory account of my book [PAF] has been accomplished to a good extent.

While preparing the manuscript, I was partially supported by the NSF grants DMS 0753991 and DMS 0854949.

Los Angeles, CA, USA Haruzo Hida

Suggestions to the Reader

In the text, articles are quoted by abbreviating the author's name; for example, articles by Hida–Tilouine are quoted as [HT1] and [HT2]. There is one exception: Articles written by the author are quoted, for example, as [H04a] and [H98], indicating also the year published (or the year written in the case of preprints). For these examples, [H04a] and [H98] are published in 2004 and in 1998, respectively. The articles by the author in a preprint form are quoted, for example, as [H13c] (though their publication year may differ from 2013). Books are quoted by abbreviating their title. For example, one of my earlier books with the title *Geometric Modular Forms and Elliptic Curves* is quoted as [GME]. Our style of reference is unconventional but has been used in my earlier books [MFG], [GME], and [PAF], and the abbreviation is (basically) common in all three books.

As for the notation and the terminology, the symbol $\mathbb{Z}_p$ denotes the p-adic integer ring inside the field $\mathbb{Q}_p$ of p-adic numbers, and the symbol $\mathbb{Z}_{(p)}$ is used to indicate the valuation ring $\mathbb{Z}_p \cap \mathbb{Q}$. Throughout the book, we indicate an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. A subfield E of $\overline{\mathbb{Q}}$ is called a number field (often assuming $[E:\mathbb{Q}] := \dim_{\mathbb{Q}} E < \infty$ tacitly). For a number field E, O_E denotes the integer ring of E, $O_{E,p} = O_E \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and $O_{E,(p)} = O_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \subset E$. A quadratic extension M/F is called a CM field if F is totally real and M is totally imaginary. For the integer ring of an imaginary quadratic field M (the simplest case of CM fields), we often use $\mathfrak{O}$ for its integer ring (in place of O_M).

The symbol $\mathcal{W}$ is exclusively used to indicate a discrete valuation ring inside $\overline{\mathbb{Q}}$ with residual characteristic p. The ring $\mathcal{W}$ could be of infinite rank over $\mathbb{Z}_{(p)}$ but with finite ramification index over $\mathbb{Z}_{(p)}$; hence, it is still discrete. The p-adic completion $\varprojlim_n \mathcal{W}/p^n\mathcal{W}$ is denoted by W, and we write $W_m = W/p^mW = \mathcal{W}/p^m\mathcal{W}$. We denote the algebraic closure $\overline{\mathbb{Q}}_p$ with p-adic absolute value $|\cdot|_p$ with $|p|_p = p^{-1}$ and write $\mathbb{C}_p$ for the completion of $\overline{\mathbb{Q}}_p$ under this absolute value. We fix two embeddings $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \subset \mathbb{C}_p$ throughout the book. We assume that $\mathcal{W} \hookrightarrow \overline{\mathbb{Q}} \xrightarrow{i_p} \mathbb{C}_p$ is continuous under the topology of the valuation ring $\mathcal{W}$; thus, we regard W as a closed subring of $\mathbb{C}_p$. For a local ring B, $\mathfrak{m}_B$ denotes its maximal ideal. We often write $\mathbb{F}$ for the residue field $\mathcal{W}/\mathfrak{m}_{\mathcal{W}} = W/\mathfrak{m}_W$.

The symbol $\mathbb{A}$ denotes the adele ring of $\mathbb{Q}$. For a subset Σ of rational primes, we set $\mathbb{A}^{(\Sigma\infty)} = \{x \in \mathbb{A} | x_\infty = x_p = 0 \text{ for } p \in \Sigma\}$. If Σ is empty, $\mathbb{A}^{(\infty)}$ denotes the ring of finite adeles. We put $\mathbb{Z}_\Sigma = \prod_{p\in\Sigma} \mathbb{Z}_p$ and define $\mathbb{Z}_{(\Sigma)} = \mathbb{Z}_\Sigma \cap \mathbb{Q}$. If $\Sigma = \{p\}$ for a prime p, we write $\mathbb{A}^{(p\infty)}$ for $\mathbb{A}^{(\Sigma\infty)}$. For a vector space of a number field E, we write $V_{\mathbb{A}} = V(\mathbb{A})$ and $V_{\mathbb{A}^{(\Sigma\infty)}} = V(\mathbb{A}^{(\Sigma\infty)})$ for $V \otimes_{\mathbb{Q}} \mathbb{A}$ and $V \otimes_{\mathbb{Q}} \mathbb{A}^{(\Sigma\infty)}$, respectively. We identify ${\mathbb{A}^{(\Sigma\infty)}}^\times$ with the subgroup of ideles $x \in \mathbb{A}^\times$ with $x_v = 1$ for $v \in \Sigma \sqcup \{\infty\}$ in an obvious way. The maximal compact subring of $\mathbb{A}^{(\infty)}$ is denoted by $\widehat{\mathbb{Z}}$, which is identified with the profinite ring $\prod_p \mathbb{Z}_p = \varprojlim_N \mathbb{Z}/N\mathbb{Z}$. We put $\widehat{\mathbb{Z}}^{(\Sigma)} = \widehat{\mathbb{Z}} \cap \mathbb{A}^{(\Sigma\infty)}$ and $\widehat{\mathbb{Z}}^{(p)} = \widehat{\mathbb{Z}} \cap \mathbb{A}^{(p\infty)}$. For a

module L of finite type, we write $\widehat{L} = L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = \varprojlim_N L/NL$, $\widehat{L}^{(\Sigma)} = L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(\Sigma)}$, and $\widehat{L}^{(p)} = L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p)}$.

An algebraic group T (defined over a subring A of $\overline{\mathbb{Q}}$) is called a torus if its scalar extension $T_{/\overline{\mathbb{Q}}} = T \otimes_R \overline{\mathbb{Q}}$ is isomorphic to a product $\mathbb{G}_m^r$ of copies of the multiplicative group $\mathbb{G}_m$. The character group $X^*(T) = \mathrm{Hom}_{\text{alg-gp}}(T_{/\overline{\mathbb{Q}}}, \mathbb{G}_{m/\overline{\mathbb{Q}}})$ is sometimes simply denoted by $X(T)$, and elements of $X(T)$ are often called weights of T. We write $X_*(T)$ for the cocharacter group $\mathrm{Hom}_{\text{alg-gp}}(\mathbb{G}_{m/\overline{\mathbb{Q}}}, T_{/\overline{\mathbb{Q}}})$. Similarly, for a split formal torus $\widehat{T}$ (see Sect. 4.4.3 for formal groups), we write $X^*(T) = \mathrm{Hom}_{\text{formal-gp}}(\widehat{T}_{/B}, \widehat{\mathbb{G}}_{m/B})$ (formal character group) and $X_*(T) = \mathrm{Hom}_{\text{formal-gp}}(\widehat{\mathbb{G}}_{m/B}, \widehat{T}_{/B})$ (formal cocharacter group). Here B is either an algebraic closure of the finite field $\mathbb{F}_p$ with p elements or the discrete valuation ring W as above, and $\widehat{\mathbb{G}}_m$ is the formal multiplicative group over B we describe later in this book.

As we will describe in Chap. 4, a scheme X can be considered either a local ringed space or a functor from a category of algebras or schemes into sets. If we want to indicate that we are thinking of X as a functor, we often write the functor as $\underline{X}$ (although we remove the underline if it is clear from the context). Similarly, for a morphism $f : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ of affine schemes, the corresponding algebra homomorphism $B \to A$ is sometimes written as $\underline{f}$ or f^* or $f^{\#}$, depending on the setting.

Contents