IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL MONOGRAPHS

Volume 242

Number Theory 3

Iwasawa Theory and Modular Forms

Nobushige Kurokawa
Masato Kurihara
Takeshi Saito

American Mathematical Society

10.1090/mmono/242

IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 242

Number Theory 3

Iwasawa Theory and Modular Forms

Nobushige Kurokawa
Masato Kurihara
Takeshi Saito

Translated from the Japanese by
Masato Kuwata

American Mathematical Society
Providence, Rhode Island

数 論 3

岩澤理論と保型形式

黒川信重・栗原将人・斎藤毅 著

SŪRON (Number Theory 3)

by Nobushige Kurokawa, Masato Kurihara, and Takeshi Saito

with financial support
from the Japan Association for Mathematical Sciences

Originally published in Japanese
by Iwanami Shoten, Publishers, Tokyo, 1998 and 2005

Translated from the Japanese by Masato Kuwata

2010 *Mathematics Subject Classification.* Primary 11–01; Secondary 11Mxx, 11R23, 11Rxx, 11Sxx, 11G05, 11Fxx.

Library of Congress Cataloging-in-Publication Data

Kurokawa, N. (Nobushige)
[Sūron. English]
Number theory 3 /Nobushige Kurokawa, Masato Kurihara, Takeshi Saito.
p. cm. — (Translations of mathematical monographs, ISSN 0065-9282; v. 242) (Iwanami series in modern mathematics)
Includes index.
Contents: v. 3. Iwasawa theory and modular forms
ISBN 978-0-8218-1355-3 (v. 3. : acid-free)
1. Number theory I. Kurokawa, Nobushige, 1952– . II. Saitō, Takeshi, 1961– . III. Title. IV. Series. V. Series: Iwanami series in modern mathematics.
QA241.K36513 2012
512′.7–dc21 99-33556
CIP

10 9 8 7 6 5 4 3 2 1 17 16 15 14 13 12

Contents

Contents, Number Theory 2

Contents, Number Theory 1

Preface

The source of the charm of number theory is the wonder of prime numbers. To elucidate the mystery of prime numbers, number theorists have made various approaches. In *Number Theory 1 and 2*, we saw ζ functions and class field theory as examples of such approaches. In this volume we continue to introduce fundamental methods of modern number theory.

One characteristic of modern number theory is the intertwinement of algebra and analysis. Algebraic entities are Galois groups and algebraic geometric objects, and analytic entities are ζ functions, modular forms, and automorphic representations. For example, the heart of class field theory, established by Teiji Takagi, may be expressed as follows: The one-dimensional representation of Galois group, an algebraic entity, and the one-dimensional representation of idele class group (Hecke character), an analytic entity, have the same ζ function. In this volume we introduce Iwasawa theory, in which an analytic entity called a p-adic L-function, a p-adic incarnation of ζ function, appears. Its algebraic and arithmetic significance will be revealed.

A generalization of class field theory to the case of nonabelian Galois groups, called "nonabelian class field theory", is one of the main themes of modern number theory which is still under construction. Its first example is the correspondence between elliptic curves, an algebraic entity, and modular forms of congruent subgroups of the modular group, an analytic entity. By establishing this correspondence Andrew Wiles proved Fermat's Last Theorem in 1995, more than 350 years after it was first proposed.

With these trends in modern number theory as a background, we introduce the fundamentals of the theory of modular forms and Iwasawa theory. We also describe the arithmetic of elliptic curves by giving an outline of the proof of Fermat's Last Theorem by Wiles.

Each chapter provides explicit calculations of examples to enhance understanding. We hope readers will compute several examples and equations by themselves so that they can experience modern number theory.

Nobushige Kurokawa, Masato Kurihara, Takeshi Saito

Preface to the English Edition

This is the English translation of the Japanese book *Number Theory 3*, the third of three volumes in the "Number Theory"series. The original Japanese book was published in 1998 (the second edition in 2005). Instead of Kazuya Kato, who co-wrote "*Number Theory 1 and 2*", Masato Kurihara is the co-author of *Number Theory 3*.

In this volume, we study modular forms and Iwasawa theory, which are very important subjects in modern number theory. (See the Objectives and Outlines of These books section of this book for the details.) As in *Number Theory 1 and 2*, we explain these theories with many concrete examples for non-specialists and beginners. In the final chapter we begin with the basics of the arithmetic of elliptic curves and give a brief exposition of a proof of Fermat's Last Theorem by Wiles. The authors hope that readers enjoy the wonderful world of modern number theory.

Nobushige Kurokawa, Masato Kurihara, Takeshi Saito

Objectives and Outline of These Books

In this volume, based on the foundations established by *Number Theory 1 and 2*, we move on to two principal themes of modern number theory. These are the theory of modular forms and Iwasawa theory. The former has an analytic aspect, while the latter has an algebraic aspect.

We describe the theory of modular forms in Chapters 9 and 11. In Chapter 9, we try to prove several beautiful relations discovered by Ramanujan and study modular forms for the modular group. In particular, we study Eisenstein series and cusp forms. Also, we introduce ζ-regularized products, and we prove Kronecker's limit formula. Here, what is essential is the automorphy of modular forms. Having the automorphy is equivalent to satisfying a certain functional equation. This is so strong a condition that the explicit shape of a modular form can be determined by it. We gather together the automorphy and Kronecker's limit formula to prove Ramanujan's relations. In Chapter 11 we view modular forms from a wider point of view and we give perspective to the automorphic form on groups and the Selberg trace formula.

Iwasawa theory is described in Chapter 10. We explain classical Iwasawa theory, especially the Iwasawa main conjecture as plainly as possible. Among the values of ζ function at the integers there are p-adic relations. This phenomenon can be clearly understood through the p-adic L-functions. We first explain the p-adic L-functions (§10.1), and then we describe Iwasawa's theory of $\mathbb{Z}_p$-extensions (§10.2). Here, we study the ideal class group, which is a very important arithmetic object, including the action of Galois group. In particular, we study the ideal class group of $\mathbb{Z}_p$-extensions, which can be thought of as the Galois group of the maximal unramified abelian extension through class field theory. Then, the results of §10.1 and §10.2 will be united by the Iwasawa main conjecture (§10.3). In Chapter 12 we describe

the basics of the arithmetic of elliptic curves, and we give a very brief account of the outline and ideas of the proof of Fermat's Last Theorem.

We hope readers will appreciate the beauty of modern number theory through this book and make their way toward the active frontier of research in number theory, using this book as a steppingstone.

Bibliography

Number fields and algebraic number theory

[1] Jean-Pierre Serre, *A course in arithmetic*. Translated from the French. Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York, 1973,

[2] André Weil, *Number theory*. An approach through history from Hammurapi to Legendre. Reprint of the 1984 edition. Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007.

[3] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, Academic Press, London, 1967.

[4] Richard Dedekind, *Theory of algebraic integers*. Translated from the 1877 French original and with an introduction by John Stillwell. Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1996.

[5] Jean-Pierre Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979.

Elliptic curves

[1] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[2] Dale Husemöller, *Elliptic curves*. Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004.

[3] Neal Koblitz, *Introduction to elliptic curves and modular forms*. Second edition. Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.

[4] Joseph H. Silverman, *The arithmetic of elliptic curves*. Second edition. Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[5] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[6] Jean-Pierre Serre, *Lectures on the Mordell–Weil theorem*. Third edition. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[7] Gary Cornell, Joseph H. Silverman, and Glenn Stevens (eds.), *Modular forms and Fermat's last theorem*. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995. Springer-Verlag, New York, 1997.

ζ functions

[1] André Weil, *Basic number theory*. Reprint of the second (1973) edition. Classics in Mathematics, Springer-Verlag, Berlin, 1995.

[2] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union., Academic Press, London, 1967.

[3] Serge Lang, *Algebraic number theory*. Second edition. Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[4] E. C. Titchmarsh, *The theory of the Riemann zeta-function*. Second edition. Edited and with a preface by D. R. Heath-Brown. The Clarendon Press Oxford University Press, New York, 1986.

[5] H. M. Edwards, *Riemann's zeta function*. Reprint of the 1974 original [Academic Press, New York]. Dover Publications Inc., Mineola, NY, 2001.

[6] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*. With the collaboration of Willem Kuyk and John Labute. Revised reprint of the 1968 original. Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998,

Class field theory

[1] Teiji Takagi, *Daisûteki Seisûron. Gaisetsu oyobi Ruitairon* (Japanese) [Algebraic number theory. Generalities and class field theory], Iwanami Shoten, Tokyo, 1948.

[2] N. Bourbaki, *Éléments de mathématique. Livre II: Algèbre. Chapitre 8: Modules et anneaux semi-simples*, Actualités Sci. Ind. no. 1261, Hermann, Paris, 1958.

[3] Emil Artin and John Tate, *Class field theory*. Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009.

[4] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, Academic Press, London, 1967.

[5] David A. Cox, *Primes of the form $x^2 + ny^2$*. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989.

[6] Jean-Pierre Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979.

[7] André Weil, *Basic number theory*. Reprint of the second (1973) edition. Classics in Mathematics, Springer-Verlag, Berlin, 1995.

Modular forms

[1] G. H. Hardy, *Ramanujan. Twelve lectures on subjects suggested by his life and work*, Cambridge University Press, Cambridge, England, 1940.

[2] I. M. Gel′fand, M. I. Graev, and I. I. Pyatetskii-Shapiro, *Representation theory and automorphic functions*. Translated from the Russian by K. A. Hirsch. Reprint of the 1969

edition. Generalized Functions, vol. 6, Academic Press Inc., Boston, MA, 1990.

[3] Andrew Ogg, *Modular forms and Dirichlet series*, W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[4] R. P. Langlands, *Problems in the theory of automorphic forms*, Lectures in modern analysis and applications, III, pp. 18–61. Lecture Notes in Math., vol. 170, Springer, Berlin, 1970.

[5] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, vol. 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[6] Roger Godement and Hervé Jacquet, *Zeta functions of simple algebras*, Lecture Notes in Mathematics, vol. 260, Springer-Verlag, Berlin, 1972.

[7] Serge Lang, *Introduction to modular forms*. With appendixes by D. Zagier and Walter Feit. Corrected reprint of the 1976 original. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 222, Springer-Verlag, Berlin, 1995.

[8] Hervé Jacquet and Joseph A. Shalika, *A non-vanishing theorem for zeta functions of* GL_n, Invent. Math. **38** (1976/77), no. 1, 1–16.

[9] Neal Koblitz, *Introduction to elliptic curves and modular forms*. Second edition. Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.

[10] Stephen Gelbart, *An elementary introduction to the Langlands program*, Bull. Amer. Math. Soc. (N.S.) **10** (1984), no. 2, 177–219.

[11] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.

[12] Daniel Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997.

[13] T. N. Bailey and A. W. Knapp (eds.), *Representation theory and automorphic forms*. Papers from the Instructional Conference held in Edinburgh, March 17–29, 1996. Proceedings of Symposia in Pure Mathematics, vol. 61, American Mathematical Society, Providence, RI, 1997.

[14] Jean-Pierre Serre, *A course in arithmetic*. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York, 1973.

Iwasawa theory

[1] Kenkichi Iwasawa, *Lectures on p-adic L-functions*. Annals of Mathematics Studies, No. 74. Princeton University Press, Princeton, N.J., 1972.

[2] Lawrence C. Washington, *Introduction to cyclotomic fields*. Second edition. Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[3] Serge Lang, *Cyclotomic fields I and II*. Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990.

[4] J. Coates, R. Greenberg, B. Mazur, and I. Satake (eds.), *Algebraic number theory*. Papers in honor of K. Iwasawa on the occasion of his 70th birthday on September 11, 1987. Advanced Studies in Pure Mathematics, vol. 17, Academic Press Inc., Boston, MA, 1989.

Answers to Questions

Chapter 10

10.1. By Proposition 10.3(2)(a), D_r is divisible by 2 and 3. Also, by (2)(b), D_r is divisible by 4.

10.2. According to the decomposition $\mathbb{Z}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$, write $a = (a_1, a_2)$ with $a_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a_2 \in 1+p\mathbb{Z}_p$. By definition $a = \omega(a_1)a_2 = \omega(a)a_2$. Since $a^{p^n} = \omega(a)a_2^{p^n}$ and $\lim_{n\to\infty} x^{p^n} = 1$ for any $x \in 1+p\mathbb{Z}_p$, we obtain $\lim_{n\to\infty} a^{p^n} = \omega(a) \lim_{n\to\infty} a_2^{p^n} = \omega(a)$. For $p = 2$, it suffices to follow the definition.

10.3. Prove by induction on n, for example.

10.4. Consider the same power series expansion as the proof of Proposition 10.5

$$L_p(s, \omega^{r_0}) = \sum_{i=0}^{\infty} a_i (s - 1 + r_0)^i.$$

By Proposition 10.8, a_i is divisible by p^2 for all $i \geq 2$. Also, since A_1 is divisible by p, a_1 is divisible by p^2 too. Then the assertion follows from the same argument as the proof of Proposition 10.5.

10.5. Identify $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_N)]]$ with $\mathbb{Z}_p[[T]]$ by associating γ' with $1+T$. If $Y \simeq \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_N)]]/(\gamma' - 1 - p)$, we have

$$\begin{aligned} Y/(1 + \gamma' + \cdots + (\gamma')^{p^n-1})Y &\simeq \mathbb{Z}_p[[T]]/(T - p, ((1+T)^{p^n} - 1)/T) \\ &\simeq \mathbb{Z}_p/2p^n\mathbb{Z}_p \end{aligned}$$

for $n \geq 1$. Thus, by Lemma 10.30, we have

$$\#A_{K_n} = \#(X/Y) + \#(\mathbb{Z}_p/2p^{n-N}\mathbb{Z}_p)$$

for $n > N$, and thus Iwasawa's formula holds. In particular, we have $\mu = 0$, $\lambda = 1$ in this case.

If $Y \simeq \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K_N)]]/((\gamma'-1)^2-p)$, then we have

$$Y/(1+\gamma'+\cdots+(\gamma')^{p^n-1})Y \simeq \mathbb{Z}_p[[T]]/(T^2-p,((1+T)^{p^n}-1)/T) \simeq \mathbb{Z}_p[\sqrt{p}]/(p^n)$$

for $n \geq 1$ if p is odd, and $n \geq 2$ if $p = 2$. Thus, we have

$$\#A_{K_n} = \#(X/Y) + p^{2(n-N)}$$

for at least $n > N+1$, and thus Iwasawa's formula holds. In particular, we have $\mu = 0$, $\lambda = 2$ in this case.

10.6. (1) If $\lambda(G_{\omega^{1-i}}(T)) > 1$, then by Question 4, we have $\zeta(1+i-p) \cong \zeta(2+i-2p) \bmod p^2$.
(2) It can be verified using the values shown in §10.1(1).
(3) Omitted.

10.7. $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ acts on $(\mathbb{Z}/p^n\mathbb{Z})(r)$ by the multiplication by $\kappa(\sigma)^r$. Considering the fact $\#(\mathbb{Z}/p^n\mathbb{Z})^\times = (p-1)p^{n-1}$, we have

$$\#\big((\mathbb{Z}/p^n\mathbb{Z})(r)\big)^{\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})} = p^n \iff (p-1)p^{n-1} \mid r.$$

The assertion follows from this.

Chapter 12

12.1. Given an odd prime number l, we regard $E : y^2 = x^3 - x$ as an elliptic curve over $\mathbb{F}_l$. E has four 2-torsion points, and thus $E(\mathbb{F}_l)$ has a subgroup of order 4. Thus the order of $E(\mathbb{F}_l)$ is divisible by 4.

Answers to Exercises

Chapter 9

9.1. (1), (2), (3) can be obtained respectively by comparing the Fourier coefficients of $E_4^2 = E_8$, $E_4E_6 = E_{10}$, $1728\Delta = E_4E_8 - E_6^2$. For example, $E_4E_6 = E_{10}$ is written as

$$\Big(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\Big)\Big(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\Big) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n,$$

and by comparing the coefficients of q^n of both sides, we obtain

$$240\sigma_3(n) - 504\sigma_5(n) - 240\cdot 504\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m) = -264\sigma_9(n).$$

Dividing by this 24, we obtain (2).

9.2. The answer is $\frac{B_k}{2k}$, where B_k is the Bernoulli number. This can be obtained as follows. By letting $z = i$ in the transformation formula $E_k\big(-\frac{1}{z}\big) = z^kE_k(z)$ of the holomorphic Eisenstein series of weight k, we obtain $E_k(i) = i^kE_k(i) = -E_k(i)$, which implies $E_k(i) = 0$. On the other hand, we have

$$E_k(i) = 1 - \frac{k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)e^{-2\pi n} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\frac{n^{k-1}}{e^{2\pi n}-1}.$$

The answer follows from these.

9.3. (1) Taking the logarithm of the formula

$$e^{-2\pi}\prod_{n=1}^{\infty}(1-e^{-2\pi n})^{24} = \Big(\frac{\varpi}{\sqrt{2}\pi}\Big)^{12}$$

in Theorem 9.16(3), we obtain (1), (2) and (3). You may use the method of Hurwitz described in Supplement 2 of Theorem 9.16, but

direct calculations show

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^8} = 2\zeta(8)E_8(i) = 2\zeta(8)E_4(i)^2$$
$$= 2\Big(\frac{\pi^8}{9450}\Big)\cdot 9\Big(\frac{\varpi}{\pi}\Big) = \frac{\varpi^8}{525},$$

and

$$\sum_{m,n=-\infty}^{\infty}{}' \frac{1}{(m+ni)^{12}} = 2\zeta(12)E_{12}2(i)$$
$$= 2\Big(\frac{2^{10}}{13!}\cdot\frac{691}{105}\pi^{12}\Big)\Big(\frac{2^6\cdot 3^5\cdot 7^2}{691}\cdot\frac{\varpi^{12}}{2^6\pi^{12}}\Big) = \frac{2\varpi^{12}}{53625}.$$

Here, we calculated $E_{12}(i)$ by letting $z = i$ in the formula

$$E_{12} - E_6^2 = \frac{2^6\cdot 3^5\cdot 7^2}{691}\Delta$$

in §9.1(b), and using the value of $\Delta(i)$ given in Theorem 9.16(3).

9.4. (1) Since $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, we have

$$E_k\Big(\frac{-1}{z+1}\Big) = (z+1)^k E_k(z).$$

Letting $z = \rho$ and using the fact $\dfrac{-1}{\rho+1} = \rho$ and $\rho + 1 = -\rho^2$, we obtain

$$E_k(\rho) = \rho^{2k}E_k(\rho).$$

Thus, if $3 \nmid k$, we have $E_k(\rho) = 0$. In particular $E_4(\rho) = 0$. Thus, letting $z = \rho$ in the formula $\Delta = \dfrac{E_4^3 - E_6^2}{1728}$, we obtain

$$E_6^2(\rho)^2 = -1728\Delta(\rho) = 1728e^{-\sqrt{3}\pi}\prod_{n=1}^{\infty}\big(1-(-1)^n e^{-\sqrt{3}\pi n}\big)^{24},$$

which shows $E_6(\rho) \neq 0$.

(2) Since we have

$$E_k(\rho) = 1 + \frac{2k}{B_k}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n} + (-1)^{n-1}},$$

and $E_k(\rho) = 0$ if $3 \nmid k$, we have

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}n^{k-1}}{e^{\sqrt{3}\pi n} + (-1)^{n-1}} = -\frac{B_k}{2k}.$$

This answers the case $k = 4$ and $k = 8$. For $k = 2$, letting $z = \rho$ in the transformation formula

$$E_2\Big(\frac{-1}{z+1}\Big) = (z+1)^2 E_2(z) + \frac{6(z+1)}{\pi i}$$

(see §9.5(e)), we obtain

$$E_2(\rho) = \frac{2\sqrt{3}}{\pi}.$$

Thus we have

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1} n^{k-1}}{e^{\sqrt{3}\pi n} + (-1)^{n-1}} = \frac{\sqrt{3}}{12\pi} - \frac{1}{24}.$$

9.5. (i) $\Leftrightarrow$ (ii) is clear. We show (ii) $\Rightarrow$ (iii), (iii) $\Rightarrow$ (iv), and (iv) $\Rightarrow$ (i).

(ii) $\Rightarrow$ (iii). From the recurrence formula, we have

$$\tau(p^l) = p^{\frac{11}{2}l} \frac{\sin(l+1)\theta_p}{\sin\theta_p}.$$

Thus we see

$$|\tau(p^l)| \le p^{\frac{11}{2}l}(l+1).$$

Therefore, if we write $n = \prod_p p^{l(p)}$, then we have

$$|\tau(n)| = \prod_p |\tau(p^{l(p)})| \le \prod_p p^{\frac{11}{2}l(p)}(l(p)+1) = n^{\frac{11}{2}} d(n).$$

(iii) $\Rightarrow$ (iv) This follows from the fact $d(n) = O(n^{\varepsilon})$.

(iv) $\Rightarrow$ (i) We show its contrapositive. Suppose there is a prime p such that $|\tau(p)| > 2p^{\frac{11}{2}}$. Then, there is a real number α such that $|\alpha| > 1$ and

$$1 - \tau(p)u + p^{11}u^2 = (1 - p^{\frac{11}{2}}\alpha u)(1 - p^{\frac{11}{2}}\alpha^{-1}u).$$

Now, if we let $\varepsilon = \frac{1}{2}\log_p|\alpha| > 0$, then we see that $\frac{\tau(n)}{n^{\frac{11}{2}+\varepsilon}}$ is not bounded. Indeed, since $|\frac{\alpha}{p^{\varepsilon}}| = \sqrt{|\alpha|} > 1$,

$$\frac{\tau(p^l)}{p^{l(\frac{11}{2}+\varepsilon)}} = \frac{1}{p^{l\varepsilon}} \cdot \frac{\alpha^{l+1} - \alpha^{-(l+1)}}{\alpha - \alpha^{-1}}$$

is not bounded as $l \to \infty$.

9.6. Let r_1 be the number of real places of K and r_2 the number of complex places. Then, the Taylor expansion formula of $\zeta_K(s)$ at $s = 0$ takes the form

$$\zeta_K(s) = -\frac{Rh}{w} s^{r_1+r_2-1} + \cdots$$

(see Theorem 7.10(4) in Chapter 7 of *Number Theory 2*). We divide into three cases.

(i) $r_1 + r_2 = 1$. Namely, $(r_1, r_2) = (1,0), (0,1)$ ($K = \mathbb{Q}$ or imaginary quadratic field.)

(ii) $r_1 + r_2 = 2$. Namely, $(r_1, r_2) = (2,0), (1,1), (0,2)$ (K is a real quadratic field, a cubic field such as $\mathbb{Q}(\sqrt[3]{2})$, or a quartic field such as $\mathbb{Q}(\zeta_5)$.)

(iii) $r_1 + r_2 \geq 3$. The rest.

First, in the case (iii), we have $\zeta_K'(0) = 0$, and thus $\prod_{\mathfrak{a}} N(\mathfrak{a}) = 1$.

(i) If $K = \mathbb{Q}$, then by Corollary 9.13, we have

$$\zeta_{\mathbb{Q}}'(0) = -\frac{1}{2}\log(2\pi).$$

Thus we have

$$\prod_{\mathfrak{a}} N(\mathfrak{a}) = \prod_{n=1}^{\infty} n = \sqrt{2\pi}.$$

If $K = \mathbb{Q}(\sqrt{-1})$, then by Theorem 9.16(2) we have

$$\zeta_{\mathbb{Q}(\sqrt{-1})}'(0) = -\frac{1}{4}\log\left(\frac{\Gamma(\frac{1}{4})^4}{4\pi}\right).$$

Thus

$$\prod_{\mathfrak{a}} N(\mathfrak{a}) = \Big(\prod_{m,n=-\infty}^{\infty}{}' (m^2+n^2)\Big)^{\frac{1}{4}} = 2^{-\frac{1}{2}}\pi^{-\frac{1}{4}}\Gamma\Big(\frac{1}{4}\Big) = 2^{\frac{1}{4}}\varpi^{\frac{1}{2}}.$$

In the case of imaginary quadratic fields in general, a similar method can be applied (see the results of Lerch (1987) and Chowla-Selberg (1949/1964)).

In the case of (ii), the rank of the unit group is 1, and we can write $R = \log|\varepsilon|$, where ε is the fundamental unit satisfying $|\varepsilon| > 1$. Thus we have

$$\zeta_K'(0) = -\frac{h}{w}\log|\varepsilon|.$$

Hence we obtain

$$\prod_{\mathfrak{a}} N(\mathfrak{a}) = |\varepsilon|^{\frac{h}{w}}.$$

Note that this is an algebraic integer.

Chapter 10

10.1. Since the numerators of $\zeta(-1), \dots, \zeta(-9)$ are not divisible by p, it follows from Corollary 10.38 that

$$A_{\mathbb{Q}(\mu_p)}^{\omega^{p-2}} = \cdots = A_{\mathbb{Q}(\mu_p)}^{\omega^{p-10}} = 0.$$

Thus, by Theorem 10.36(1), we have

$$X^{\omega^{p-2}} = \cdots = X^{\omega^{p-10}} = 0.$$

10.2. (1) We may assume $r > 2$. Expanding into a power series $L_p(s, \omega^r) = \sum_{i=0}^{\infty} a_i (s-1+r)^i$, we have

$$\zeta(1-r) \equiv L_p(1-r, \omega^r) = a_0 \mod p^2.$$

Since by Proposition 10.8, a_i is divisible by p^2 for $i \geq 2$, we have

$$\zeta(2-r-p) \equiv L_p(2-r-p, \omega^r) \equiv a_0 + a_1(1-p) \mod p^2.$$

Thus we have

$$a_1 \equiv \big(\zeta(2-r-p) - \zeta(1-r)\big)/(1-p) \mod p^2,$$

and we see

$$\begin{aligned} L_p(0, \omega^r) &\equiv a_0 + a_1(r-1) \\ &\equiv \big((2-r-p)\zeta(1-r) - (1-r)\zeta(2-r-p)\big)/(1-p) \not\equiv 0 \mod p^2. \end{aligned}$$

Hence we have $\mathrm{ord}_p(L(0, \omega^{r-1})) = \mathrm{ord}_p(L_p(0, \omega^r)) = 1$. The assertion now follows from Theorem 10.37.

(2) It can be verified by using the values of the zeta function in §10.1 (a).

10.3. (1) From the Iwasawa main conjecture, we see that X^{ω^i} is a free $\mathbb{Z}_p$-module of rank 1. Thus X^{ω^i} is generated by one element over $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p))]] \simeq \mathbb{Z}_p[[T]]$, and thus we can write as $X^{\omega^i} \simeq \Lambda/(G_{\omega^{1-i}}(T))$. By the definition of associated polynomial, we have $\mathrm{ord}_p(\alpha) > 0$. The assertion now follows from Theorem 10.36 in a similar manner to that of Question 5.

(2) X^{ω^i} is a free $\mathbb{Z}_p$-module of rank 2 by the Iwasawa main conjecture.

(i) The case where X^{ω^i} is generated by one element over Λ. In this case we have

$$X^{\omega^i} \simeq \Lambda/(G_{w^{1-i}}(T)) \simeq \Lambda/((T-\alpha)(T-\beta)).$$

If we put $K_n = \mathbb{Q}(\mu_{p^n})$, then by Theorem 10.36 we have

$$A_{K_n}^{\omega^i} \simeq \Lambda/((T-\alpha)(T-\beta), (1+T)^{p^{n-1}} - 1)$$

for $n \geq 1$. Using $\mathrm{ord}_p(\alpha) < \mathrm{ord}_p(\beta)$, we obtain

$$A_{K_n} \simeq \mathbb{Z}_p/\alpha\beta p^{n-1}\mathbb{Z}_p \oplus \mathbb{Z}_p/p^{n-1}\mathbb{Z}_p.$$

(ii) The case where X^{ω^i} is not generated by one element over Λ. In this case X^{ω^i} is generated by two elements over Λ. We have an exact sequence of Λ-modules of the form

$$0 \to \Lambda^2 \xrightarrow{f} \Lambda^2 \to X^{\omega^i} \to 0.$$

Let A be the matrix corresponding to f. Using the facts $\mathrm{ord}_p(\alpha-\beta)=1$ and $\mathrm{ord}_p(\alpha)<\mathrm{ord}_p(\beta)$, A can be transformed to the form $\begin{pmatrix} T-\alpha & 0 \\ 0 & T-\beta \end{pmatrix}$ by elementary transformations. Thus we have

$$X^{\omega^i} \simeq \Lambda/(T-\alpha) \oplus \Lambda/(T-\beta),$$

and

$$A_{K_n} \simeq \mathbb{Z}_p/\alpha p^{n-1}\mathbb{Z}_p \oplus \mathbb{Z}_p/\beta p^{n-1}\mathbb{Z}_p.$$

10.4. (1) The injectivity can be proved in the same way it was proved in Proposition 10.33. To show the surjectivity, use the fact

$$\Big(\bigoplus_{v\in S}\mathbb{Z}_p v\Big)^{\chi} = \Big(\bigoplus_{v\in S}\mathbb{Z}_p v\Big) \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]} \mathcal{O}_\chi = 0,$$

where S is the set of all prime ideals of F_n ramified in K_n/F_n.

(2) We can show it in a similar manner to that of Theorem 10.37.

Index

This is the third of three related volumes on number theory. (The first two volumes were also published in the Iwanami Series in Modern Mathematics, as volumes 186 and 240.)

The two main topics of this book are Iwasawa theory and modular forms. The presentation of the theory of modular forms starts with several beautiful relations discovered by Ramanujan and leads to a discussion of several important ingredients, including the zeta-regularized products, Kronecker's limit formula, and the Selberg trace formula. The presentation of Iwasawa theory focuses on the Iwasawa main conjecture, which establishes far-reaching relations between a p-adic analytic zeta function and a determinant defined from a Galois action on some ideal class groups. This book also contains a short exposition on the arithmetic of elliptic curves and the proof of Fermat's last theorem by Wiles.

Together with the first two volumes, this book is a good resource for anyone learning or teaching modern algebraic number theory.

For additional information
and updates on this book, visit

www.ams.org/bookpages/mmono-242

ISBN 978-0-8218-2095-7

9 780821 820957

MMONO/242