IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 243

Fermat's Last Theorem

Basic Tools

Takeshi Saito

American Mathematical Society

IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 243

Fermat's Last Theorem

Basic Tools

Takeshi Saito

Translated from the Japanese by
Masato Kuwata

American Mathematical Society
Providence, Rhode Island

FERUMA YOSO (Fermat Conjecture)

フェルマー予想

by Takeshi Saito

斎藤　毅

First published 2009 by Iwanami Shoten, Publishers, Tokyo.
This English language edition published in 2013
by the American Mathematical Society, Providence
by arrangement with the author c/o Iwanami Shoten, Publishers, Tokyo
Translated from the Japanese by Masato Kuwata

2010 *Mathematics Subject Classification.* Primary 11D41;
Secondary 11G05, 11F11, 11F80, 11G18.

Library of Congress Cataloging-in-Publication Data

Saito, Takeshi, 1961–
Fermat's last theorem: basic tools / Takeshi Saito ; translated by Masato Kuwata.—English language edition.
pages cm.—(Translations of mathematical monographs ; volume 243)
First published by Iwanami Shoten, Publishers, Tokyo, 2009.
Includes bibliographical references and index.
ISBN 978-0-8218-9848-2 (alk. paper)
1. Fermat's last theorem. 2. Number theory. 3. Algebraic number theory. I. Title. II. Title: Fermat's last theorem: basic tools.

QA244.S2513 2013
512.7'4–dc23

2013023932

10 9 8 7 6 5 4 3 2 1　　18 17 16 15 14 13

Fermat's Last Theorem

Basic Tools

Preface

It has been more than 350 years since Pierre de Fermat wrote in the margin of his copy of *Arithmetica* of Diophantus:

> It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree; I have discovered a truly remarkable proof which this margin is too small to contain.[1]

This is what we call Fermat's Last Theorem. It is certain that he has a proof in the case of cubes and biquadrates (i.e., fourth powers), but it is now widely believed that he did not have a proof in the higher degree cases. After enormous effort made by a great number of mathematicians, Fermat's Last Theorem was finally proved by Andrew Wiles and Richard Taylor in 1994.

The purpose of this book is to give a comprehensive account of the proof of Fermat's Last Theorem. Although Wiles's proof is based on very natural ideas, its framework is quite complex, some parts of it are very technical, and it employs many different notions in mathematics. In this book I included parts that explain the outline of what follows before introducing new notions or formulating the proof formally. Chapter 0 and §§5.1, 5.5, and 5.6 in Chapter 5 are those parts. Logically speaking, these are not necessary, but I included these in order to promote better understanding. Despite the aim of this book, I could not prove every single proposition and theorem. For the omitted proofs please consult the references indicated at the end of the book.

The content of this book is as follows. We first describe the rough outline of the proof. We relate Fermat's Last Theorem with elliptic

[1] Written originally in Latin. English translation is taken from Dickson, L. E., *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

curves, modular forms, and Galois representations. Using these relations, we reduce Fermat's Last Theorem to the modularity of certain ℓ-adic representations (Theorem 3.36) and a theorem on the level of mod ℓ representations (Theorem 3.55). Next, we introduce the notions of deformation rings and Hecke algebras, which are incarnations of Galois representations and modular forms, respectively. We then prove two theorems on commutative algebra. Using these theorems, we reduce Theorem 3.36 to certain properties of Selmer groups and Hecke modules, which are also incarnations of Galois representations and modular forms.

We then construct fundamental objects, modular curves over $\mathbf{Z}$, and the Galois representations associated with modular forms. The latter lie in the foundation of the entire proof. We also show a part of the proof of Theorem 3.55. Finally, we define the Hecke modules and the Selmer groups, and we prove Theorem 3.36, which completes the proof of Fermat's Last Theorem.

The content of each chapter is summarized at its beginning, but we introduce them here briefly. In Chapter 0, we show that Fermat's Last Theorem is derived from Theorem 0.13, which is about the connection between elliptic curves and modular forms, and Theorem 0.15, which is about the ramification and level of ℓ-torsion points of an elliptic curve. The objective of Chapters 1–4 is to understand the content of Chapter 0 more precisely. The precise formulations of Theorems 0.13 and 0.15 will be given in Chapters 1–3. In the proof presented in Chapter 0, the leading roles are played by elliptic curves, modular forms, and Galois representations, each of which will be the main theme of Chapters 1, 2, and 3. In Chapter 3, the modularity of ℓ-adic representations will be formulated in Theorem 3.36. In Chapter 4, using Theorem 4.4 on the rational points of an elliptic curve, we deduce Theorem 0.13 from Theorem 3.36. In §4.2, we review the outline of the proof of Theorem 0.1 again.

In Chapters 5–7, we describe the proof of Theorem 3.36. The principal actors in this proof are deformation rings and Hecke algebras. The roles of these rings will be explained in §5.1. In Chapter 5, using two theorems of commutative algebra, we deduce Theorem 3.36 from Theorems 5.32, 5.34, and Proposition 5.33, which concern the properties of Selmer groups and Hecke modules. The two theorems in commutative algebra will be proved in Chapter 6. In Chapter 7, we will prove the existence theorem of deformation rings.

In Chapter 8,* we will define modular curves over $\mathbf{Z}$ and study their properties. Modular forms are defined in Chapter 2 using modular curves over $\mathbf{Q}$, but their arithmetic properties are often derived from the behavior of modular curves over $\mathbf{Z}$ at each prime number. Modular curves are known to have good reduction at primes not dividing their levels, but it is particularly important to know their precise properties at the prime factors of the level. A major factor that made it possible to prove Fermat's Last Theorem within the twentieth century is that properties of modular curves over $\mathbf{Z}$ had been studied intensively. We hope the reader will appreciate this fact.

In Chapter 9,* we construct Galois representations associated with modular forms using the results of Chapter 8, and prove a part of Theorem 3.55 which describes the relation between ramification and the level. Unfortunately, however, we could not describe the celebrated proof of Theorem 3.55 in the case of $p \equiv 1 \bmod \ell$ by K. Ribet because it requires heavy preparations, such as the p-adic uniformization of Shimura curves and the Jacquet–Langlands–Shimizu correspondence of automorphic representations.

In Chapter 10,* using results of Chapters 8 and 9, we construct Hecke modules as the completion of the singular homology groups of modular curves, and we then prove Theorem 5.32(2) and Proposition 5.33. In Chapter 11, we introduce the Galois cohomology groups and define the Selmer groups. Then we prove Theorems 5.32(1) and 5.34. The first half of Chapter 11 up to §11.3 may be read independently as an introduction to Galois cohomology and the Selmer groups.

Throughout the book, we assume general background in number theory, commutative algebra, and general theory of schemes. These are treated in other volumes in the Iwanami series: *Number Theory 1*, *2*, and *3*, *Commutative algebras and fields* (no English translation), and *Algebraic Geometry* 1 and 2. For scheme theory, we give a brief supplement in Appendix A after Chapter 7. Other prerequisites are summarized in Appendices B, C, and D at the end of the volume.* In Appendix B, we describe algebraic curves over a discrete valuation rings and semistable curves in particular, as an algebro-geometric preparation to the study of modular curves over $\mathbf{Z}$. In Appendix C, we give a linear algebraic description of finite flat commutative group

*Chapters 8, 9, and 10 along with Appendices B, C, and D will appear in *Fermat's Last Theorem: The Proof*, a forthcoming translation of the Japanese original.

schemes over $\mathbf{Z}_p$, which will be important for the study of p-adic Galois representations of p-adic fields. Finally, in Appendix D, we give a summary on the Jacobian of algebraic curves and its Néron model, which are indispensable to study the Galois representations associated with modular forms.

If we gave a proof of every single theorem or proposition in Chapters 1 and 2, it would become a whole book by itself. So, we only give proofs of important or simple properties. Please consider these chapters as a summary of known facts. Reading the chapters on elliptic curves and modular forms in *Number Theory 1,2, and 3* would also be useful to the reader.

At the end of the book, we give references for the theorems and propositions for which we could not give proofs in the main text. The interested reader can consult them for further information. We regret that we did not have room to mention the history of Fermat's Last Theorem. The reader can also refer to references at the end of the book. Due to the nature of this book, we did not cite the original paper of each theorem or proposition, and we beg the original authors for mercy.

I would be extremely gratified if more people could appreciate one of the highest achievements of the twentieth century in mathematics. I would like to express sincere gratitude to Professor Kazuya Kato for proposing that I write this book. I would also thank Masato Kurihara, Masato Kuwata, and Kazuhiro Fujiwara for useful advice. Also, particularly useful were the survey articles [**4**], [**5**], and [**24**]. I express here special thanks to their authors.

This book was based on lectures and talks at various places, including the lecture course at the University of Tokyo in the first semester of 1996, and intensive lecture courses at Tohoku University in May 1996, at Kanazawa University in September 1996, and at Nagoya University in May 1999. I would like to thank all those who attended these lectures and took notes. I would also like to thank former and current graduate students at the University of Tokyo, Keisuke Arai, Shin Hattori, and Naoki Imai, who read the earlier manuscript carefully and pointed out many mistakes. Most of the chapters up to Chapter 7 were written while I stayed at Université Paris-Nord, Max-Planck-Institut für Mathematik, and Universität Essen. I would like to thank these universities and the Institute for their hospitality and for giving me an excellent working environment.

This book is the combined edition of the two books in the Iwanami series The Development of Modern Mathematics: *Fermat's Last Theorem 1* first published in March 2000 and containing up to Chapter 7; and *Fermat's Last Theorem 2* published in February 2008.

Since 1994 when the proof was first published, the development of this subject has been remarkable: Conjecture 3.27 has been proved, and Conjecture 3.37 has almost been proved. Also, Theorem 5.22 has been generalized widely, and its proof has been simplified greatly. We should have rewritten many parts of this book to include recent developments, but we decided to wait until another opportunity arises.

On the occasion of the second edition, we made corrections to known errors. However, we believe there still remain many mistakes yet to be discovered. I apologize in advance, and would be grateful if the reader could inform me.

Takeshi Saito
Tokyo, Japan
November 2008

Preface to the English Edition

This is the first half of the English translation of *Fermat's Last Theorem* in the Iwanami series, The Development of Modern Mathematics. Though the translation is based on the second combined edition of the original Japanese book published in 2008, it will be published in two volumes. The first volume, *Fermat's Last Theorem: Basic Tools*, contains Chapters 1–7 and Appendix A. The second volume, *Fermat's Last Theorem: The Proof*, which will be published in a short while, contains Chapters 8–11 and Appendices B, C, and D.

The author hopes that, through this edition, a wider audience of readers will appreciate one of the deepest achievements of the twentieth century in mathematics.

My special thanks are due to Dr. Masato Kuwata, who not only translated the Japanese edition into English but also suggested many improvements in the text so that the present English edition is more readable than the original Japanese edition.

Takeshi Saito
Tokyo, Japan
June 2013

Contents