I was excited to hear that Takeshi Saito’s books on the proof of Fermat’s Last Theorem had been translated and appeared as two fairly thin books in the series “Translation of Mathematical Monographs” by the AMS. Richard Taylor and Andrew Wiles made this major breakthrough in the mid-nineties. Saito’s books, containing both the “Basic Tools” as well as “The Proof”, appear twenty years later with these subtitles.

The subject has lost none of its appeal and importance in the interim; on the contrary, the methods used in the proof produced numerous other important results, such as the proof of the Sato-Tate conjecture by Richard Taylor and his collaborators and the proof of Serre’s modularity conjecture by Chandrashekhar Khare and Jean-Pierre Wintenberger.

There have been quite a number of publications devoted to the mathematics involved in the the proof of Fermat’s Last Theorem. Most of them are surveys or they present the main mathematical concepts (elliptic curves, modular forms and Galois representations) involved in the proof without going into details. The conference volume [1] edited by Cornell, Silverman and Stevens and the article [2] by Darmon, Diamond and Taylor stand out as having a similar aim as the books under review. The former is a collection of very good articles, though it may lack in consistency and clear focus which is one of the strengths of Saito’s books. The latter does not cover the basic tools in as much detail and it is less self-contained. All three are best used in parallel.

The books follow the original arguments and modifications already present in [1] and [2] to a large degree. As I am not a specialist in the field myself, I cannot comment on whether with more recent methods one could simplify part of the proof. However I am certain that the two books under review provide a very good base for reading more recent articles in this active research area.

Obviously, one should not expect that the complete proof is contained in these two volumes. For instance, no reader will be surprised to see that neither Falting’s proof of the Mordell conjecture nor the proof of global duality in Galois cohomology is included. The author had to make some choices as to what prerequisites he assumes and what material he leaves out. For instance, despite the rather gentle first 25 pages, the reader needs to know quite a bit of scheme theory. Although it is not strictly necessary, it is also good if the reader is familiar with the basics theory of elliptic curves and modular forms.

In my opinion, the author makes an excellent choice as to what to include in order to obtain a coherent exposition which is as self-contained as possible. The references at the end contain precise indications on where to find the proofs which are omitted in the books. For instance, rather than including the full proof of Ribet’s level lowering theorem, only Mazur’s earlier theorem is given. The reader still gets a good grasp of how to obtain such results. The only omission I felt a bit disappointed about was the lack of discussion on the crucial result by Langlands and Tunnell. The Galois representation associated to the 3-torsion points of an elliptic curve becomes magically modular with one reference while the remaining part of the book is then about how to deduce from this the modularity of the elliptic curve itself.

Let me give an overview of the contents of
the eleven chapters of the books. The first book
starts with a synopsis containing the statement
of Fermat’s Last Theorem and an explanation of
how the modularity of the Frey curve implies it.

Then the first chapter covers elliptic curves
over arbitrary base schemes and generalised el-
liptic curves in view of the moduli problems de-
scribed later. As mentioned before, this is self-
contained but having seen a more elementary
approach before may be helpful. The follow-
ing chapter covers the basics on modular forms
of weight 2. They are systematically developed
as geometric modular forms by constructing the
modular curves as moduli spaces over \( \mathbb{Q} \)
and modular forms are defined as differentials on
them. Chapter 3 introduces Galois representa-
tions and local conditions on them. It is here
that we meet for the first time the crucial con-
dition simply called “good at \( p \)" which requires
the local representation to come from a finite flat
group scheme defined over \( \mathbb{Z} \). It is explained
when this is the case for the Galois representa-
tion attached to an elliptic curve and stated for
the Galois representation attached to a modular
form.

After having set up the three main concepts
that are involved in the proof, the next two chap-
ters give an overview of the proof and announce
the major theorems that will be proven later. In
chapter 4, the 3–5 trick explains how the mod-
ular lifting theorem implies the modularity of
semi-stable elliptic curves. An overview of the
proof of the modular lifting theorem is given in
the next chapter. It explains the meaning and
use of what is simply called \( R = T \), namely that
a certain universal deformation ring of Galois
representations is isomorphic to a certain Hecke
algebra connected to modular forms. Both of
them are described together with finer versions
\( R_\Sigma \) and \( T_\Sigma \) which impose the local restrictions on
ramification only outside a finite set \( \Sigma \) of primes.

The author defines what he calls an RTM-triple,
which consists of triples \( (R_\Sigma, T_\Sigma, M_\Sigma) \) together
with a map \( f: R_\Sigma \to T_\Sigma \). Two numerical criteria
for a ring like \( R_\Sigma \) to be a local complete inter-
section and for the map \( f \) to be an isomorphism
are stated. The first will be used to prove the
case when \( \Sigma \) is empty and the second to prove it
inductively when enlarging the set \( \Sigma \).

The first book finishes with two more technical
chapters, one on commutative algebra proving
the two criteria for local complete intersections
and the other on deformation rings of Galois rep-
resentations. In the latter the construction of the
universal deformation ring \( R_\Sigma \) is given.

The second book starts with chapter 8, which
contains a thorough and nice development of
moduli problems for elliptic curves with the aim
of constructing the modular curves as schemes
over \( \mathbb{Z} \). The curves \( Y_0(N) \) and \( Y_1(N) \), their
compactifications and the important maps be-
tween them are carefully constructed. More ex-
otic moduli problems and the Igusa curves are
also explained. They are used in the next chap-
ter which starts by constructing the Hecke alge-
bra with integer coefficients and the Galois rep-
resentation attached to a modular form. The
second part of this chapter is devoted to the level
ingoing result studying the Néron model of the
Jacobian of the modular curve.

The heart of the proof that \( R_\Sigma \) and \( T_\Sigma \) are
isomorphic is contained in the last two chapters.
First, in chapter 10, the Hecke module \( M_\Sigma \)
coming from modular symbols is defined and
analysed. The maps between modular curves
are used to compute a so-called multiplier and
show the surjectivity of a map between the Hecke
modules as \( \Sigma \) increases. Then one has to verify
the numerical criterion using a well-chosen set \( Q \)
of auxiliary primes. The final chapter introduces
Galois cohomology. The relevant Selmer groups are defined and linked to the deformation problem of Galois representations. Finally, global duality of Galois cohomology concludes the proof.

The books also have appendices with collections of results on arithmetic geometry, on the theory of Fontaine and Laffaille and on Néron models. They have good indices of notations, a complete bibliography, but they contain hardly any examples or exercises.

As I reach the conclusion of this review, I would like to mention one issue I had with these books: The logical structure is very complicated. Frequently, theorems are announced and only proven much later after they were used to deduce earlier statements. It is a matter of taste, but I would have preferred a more linear structure to these frequent flash-forwards. Sections 4.2, 5.5 and 5.6 are of much help with understanding the structure.

Another strange, yet harmless fact about the book is that it omits to attribute any of the intermediate results to the mathematicians who discovered them. Also famous buzzwords like “modularity lifting” or “level lowering” are not mentioned.

In summary, I enjoyed reading this book. The author states in his introduction “I would be extremely gratified if more people could appreciate one of the highest achievements of the twentieth century in mathematics.” These books are a very good contribution for exactly this purpose. Number theorists, including graduate students, will find the proof of Fermat’s Last Theorem and the modularity of elliptic curves and its prerequisites much more accessible thanks to these two books.

References


Christian Wuthrich
University of Nottingham
Fermat's Last Theorem can be stated simply as follows: It is impossible to separate any power higher than the second into two like powers, or, more precisely: If an integer \( n \) is greater than 2, then the equation \( a^n + b^n = c^n \) has no solutions in non-zero integers \( a, b, \) and \( c. \) If you let \( n = 2, \) the equation takes the form. Pythagoras produced by means of a combination of logic and elementary geometry a proof for every right angled triangle. He then passed from an empirical proof for a finite number of cases to a proof as we currently understand it, that is a proof that it is always true for fixed preconditions. Proofs are those which differentiate mathematics from all other sciences.