BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 36, Number 2, Pages 261–266
S 0273-0979(99)00778-8
Article electronically published on February 22, 1999

Modular forms and Fermat's Last Theorem, by G. Cornell, J. H. Silverman, and G. Stevens, Springer-Verlag, New York, 1997, xix + 582 pp., $49.95, ISBN 0-387-94609-8

1. History

The story is now well-known—in June 1993, Andrew Wiles announced, at a conference in Cambridge, a proof that every semi-stable elliptic curve over the rationals was modular. As many of the people in the audience were already aware, this result, together with another deep theorem proved by Ken Ribet in the 1980s, implied Fermat's Last Theorem. Later on in 1993, the rumour was that a gap had emerged in Wiles' proof (what was actually going on was unclear to most people, because Wiles' manuscript had still not been made public). But in October of 1994, a slightly modified paper [7] was (finally!) released, together with another paper, [6], jointly authored by Wiles and Richard Taylor, which filled in the gap, and suddenly Fermat's Last Theorem really was a theorem.

The preprints were yet another startling example of how important the methods of arithmetic algebraic geometry have become in number theory. Also packed into these papers was some deformation theory, some commutative algebra, results from the theory of modular forms and Hecke algebras, Galois cohomology, and not just one but several highly ingenious new ideas. Indeed Wiles had proved far more than "just" showing that all semi-stable elliptic curves were modular; he had proved some very clever general theorems which could be used to show that a large class of objects (certain 2-dimensional Galois representations) were related to modular forms. And so began the crucial test: would the ideas in the proofs withstand the detailed examination which many of the experts in algebraic number theory and algebraic geometry would now give them?

As time went on, people became more and more optimistic that (this time!) there did not seem to be a problem with the argument. The results in the preprints were strengthened, simplified and clarified by other mathematicians, but the argument with all its details still remained complicated, subtle, and long.

In 1995, a conference was organised by Gary Cornell, Joe Silverman and Glenn Stevens, and the subject was, essentially, the mathematics behind the proof of Wiles' results. The principle was simple—if one could attract sufficiently many experts to the same place at the same time, then there really would be a body of people who, together, could understand all of the proof, and indeed were perhaps even capable of trying to explain a lot of the mathematics going into it. Experts in one particular area could give talks on the results from this area that Wiles had used or proved. This might initially sound optimistic, but somehow the three organisers managed to round up an incredibly impressive list of speakers. Many of the experts in modern algebraic number theory were to be speakers at the conference, and many more were attending it!

The conference was ten days long, and the aim seemed to be to cover as much of the mathematics that was needed to prove Fermat's Last Theorem as possible.

1991 *Mathematics Subject Classification.* Primary 11-06.

The conference talks were supposed to be accessible to graduate students in number theory. If one had to give a one-line review of the book in question, one could say "The book is the Proceedings of this conference." But right from the start one realises that the book is not the usual kind of conference proceedings. Clearly a lot of thought has gone into giving it more structure than just a collection of articles relating to Fermat's Last Theorem. Moreover, in the preface to the book, it claims (not without good reason, in my opinion!) that the conference was "one of the largest and liveliest number theory conferences ever held." From such a conference one would perhaps hope that the proceedings were also lively! And to a large extent this is indeed the case.

2. What is the book?

Firstly, perhaps it should be made clear what the book is not. The book is certainly not a book full of anecdotes, intended for the non-mathematician. There are several such books in existence, some of them very good, but this is not one. This book is also *not* a complete proof of Fermat's Last Theorem. Even though it is nearly 600 pages long, it does not contain a proof of every result that is needed in Wiles' proof. For example, Wiles needs Ribet's result that modularity of semi-stable curves implies Fermat's Last Theorem, and for this Ribet needs Mazur's results on bounds for the torsion of elliptic curves over $\mathbb{Q}$, and essentially nothing is said about the proof of Mazur's results. To give another very important example, Wiles in his proof needs the results of Langlands and Tunnell on the relationship between modular forms and certain irreducible 2-dimensional representations of the absolute Galois group of the rationals, and although a chapter of the book is devoted to the key ideas behind the proof of the result, it would probably take another entire book to give all the details. There are several other examples that one could mention, but the point is probably already made.

So what is the book, then? Well, most of the book is an attempt to take many of the important ideas needed in the proof, and to explain these ideas in a way that makes them accessible to a graduate student in number theory. Several of these ideas were previously only explained in research papers, and others were only in the literature in a much more general form than was needed for the proof. The last few chapters are of a slightly different nature: some give certain corollaries or extensions of Wiles' main results, and others talk about the mathematical history of the Theorem and what was known before Wiles' work.

3. The articles—an overview

One thing that separates the book from a usual conference proceedings is that a lot of thought clearly has gone into making the book read more like a book than like a collection of articles on different subjects by different authors. There is continual cross-referencing between the different articles, and the editors have done a very good job of arranging the material so that many of the ideas in the proof are built from scratch.

Of course, it is hard to make any general comments about the collection of all articles in the volume. They are written by different people with different views on mathematics, that is clear. Some articles prove many of the results they need themselves, others merely give references, and still others just give an overview, not worrying so much about details. Some articles are summaries of subjects which

are already well-treated in graduate textbooks, and others are on subjects which were until now essentially only treated in research articles. Some articles are very meticulously prepared; others contain more than their fair share of misprints! As one could expect with different people writing different chapters, one is bound to run into several mathematical styles.

Overall, the standard of the articles is high. Moreover, and something which should be emphasized, one could very well be interested in this book even if one is not interested in seeing a lot of the details behind Wiles' work. This is a property of the book which brings to mind the previous book [2] by Cornell and Silverman, which was the proceedings of a conference on Faltings' proof of the Mordell conjecture. Even if one did not wish to see all the technicalities of Faltings' proof, [2] still had a lot to offer, because it contained introductory chapters on group schemes, abelian varieties, Jacobians, Néron models, and more. Similarly, in this case the authors have put together a book which will be a very useful reference for graduate students or others wanting to learn some arithmetic algebraic geometry. For example, there are articles on elliptic curves, modular curves (and modular forms), finite flat group schemes, Serre's conjecture, and several other subjects that could well be of interest to people wishing to learn something about this branch of number theory.

4. The details

Finally, here are some more details about the structure of the book, and the structure of the proof as presented in the book.

The first chapter, by Stevens, contains an overview of the proof of Fermat's Last Theorem, indicating how the big (but sometimes technical) theorems in the subject fit together to prove the result. After this, there are two "introductory" chapters, introducing readers to the main stars of the proof: one by Silverman (who better to write such an article!) on elliptic curves, and one by Rohrlich on modular curves. Although it is hard to criticise the book in general, one could perhaps suggest that maybe a third introductory chapter would have been useful here. Rohrlich's article explains the theory of modular curves over fields, which is of course essential to the proof, but in order to really work with these modular curves one is in the end forced to understand certain nice integral models of these curves over bases such as $\mathrm{Spec}(\mathbb{Z}_p)$. There is now a very well-understood theory of models of modular curves over these bases, and indeed the theory is a very good example of the power of Grothendieck's theory of schemes. The two main references for the theory of modular curves over these local base schemes are still, as far as I know, [3] and [5], and it is a shame that this continues to be the case, because neither [3] nor [5] is particularly easy reading without a good background in algebraic geometry. Clearly Rohrlich has no time to develop the integral theory in the 60 pages that he has, and hence is forced to merely refer to "work of Igusa" when, for example, talking about the Eichler-Shimura relations. Yet to follow the details of what is going on, one ultimately has to understand the integral theory, and it is a shame that very little is said about it, particularly when it is extensively used in other articles in the book. So why is there not another article dealing with the integral theory? In fact, the answer is probably that unfortunately the subject is rather technical, and is a real headache to deal with rigorously, especially when one wants to deal with the cusps (either via "normalisation" or via the theory of generalised

elliptic curves). One still pities the graduate student who has to learn about these integral models.

After these introductory lectures, the book goes on to explain some more of the "standard" theory that one will need to follow Wiles' proof. The article by Washington is a lively explanation of the Galois cohomology that Wiles needs, and then follows a fabulous article by Tate, full of insights about finite flat group schemes, with crisp, clear proofs. In fact it is hard to think of a paper where the subject of finite flat group schemes is treated more clearly.

There then follows another long article by Gelbart explaining some of the fragmentary known results concerning Langlands' conjectures and how they are enough to deduce the proof of the theorem of Langlands and Tunnell. One thing this article perhaps does not emphasize is how very deep the proofs of these fragmentary known results are! However, the reader might be able to guess—for example, Gelbart sometimes refers the reader to results in [4], and this book itself is several hundred pages long.

After this is a very clear and precise article by Edixhoven, where he sketches pretty much everything that is known about Serre's conjecture, especially the work of Ribet, and then explains carefully how one manipulates the weight 1 form obtained by the Langlands–Tunnell theorem into a weight 2 form.

After all this, we are ready to get started! There now follows a long article by Mazur and a rather shorter one by de Smit and Lenstra. Between them, these articles explain, mostly from first principles, everything that one needs to know about deformation theory to understand the construction of the deformation rings that Wiles will use in his proof. The next article, by Tilouine, sketches some essential results about Hecke rings. Finally we are in a position to write down a deformation ring R, a Hecke ring T, and a ring homomorphism $R \to T$.

One of Wiles' insights was that in many cases this ring homomorphism could be an isomorphism (which is a precise way of formulating the statement that all deformations of a certain type of a mod p Galois representation are related to modular forms). In fact, by this stage in the book we have already seen many of the details behind the proof that if this map $R \to T$ is an isomorphism, then Fermat's Last Theorem is true. So now the problem has turned into a question in the theory of commutative rings. We have already picked up various facts about the rings R and T. Now we have to understand another one of Wiles' insights—that the map between them is an isomorphism if and only if two abelian groups occurring in the theory are finite and have the same cardinality. This is the so-called "numerical criterion", or, as it is called in the article by de Smit, Rubin and Schoof, "Criterion I". Given this result, one can see that Fermat's Last Theorem is reduced to a statement saying that two groups have the same order! Also in this latter article, the authors establish an important "Criterion II" for $R \to T$ to be an isomorphism, which is to be used later.

Checking that the map $R \to T$ is an isomorphism is actually very difficult and forms the heart of Wiles' proof. Even though several good ideas have already been used, several more will be needed. The strategy is to show that the map $R \to T$ is an isomorphism in the so-called "minimal case", and then to deduce it in the general case. This last deduction is the subject of the chapter by Diamond and Ribet. This is where Criterion I comes into play. If $R = T$ in the minimal case, then by Criterion I we have that two abelian groups are finite and have the same cardinality in the minimal case. Now we use the Galois cohomology which was explained earlier in

the book, and also results of Ribet on level-raising, to deduce that Criterion I holds in the general case, and hence that $R = T$ in the general case. The authors explain this in some detail. The trick is to control the growths of the groups as one changes from the minimal case to non-minimal cases, and then one can see how equality in the minimal case implies equality in general. The calculations on how the groups change as one goes from case to case are mostly standard (given the results of Ribet), but there is one particularly subtle case, where computing the change in one of the groups involves a very subtle computation of flat deformations. In fact this computation is sufficiently deep to merit an article of its own—the chapter by Conrad, who clearly explains Fontaine's theorems on finite flat group schemes and how one can use them to explicitly carry out this computation. In fact this latter article is again an example of a good explanation of a theory which one might be independently interested in, whether or not one wants to follow Wiles' proof.

By this stage, one feels that one is nearing the goal. But the proof that the map $R \to T$ is an isomorphism in the minimal case is the part of Wiles' proof that initially was incorrect. The correct proof of the isomorphism in the minimal case is in the paper [6] and is now the main goal of the book. If the book were to be an accurate account of what actually happened in real life, then there would probably now follow 50 blank pages, representing the uncomfortable feeling that we were probably nearly there but it wasn't clear what was going to happen next. But in fact the book jumps straight to the happy ending, with the article by de Shalit, explaining Faltings' simplification of the paper by Taylor and Wiles, and how Criterion II was established in the minimal case. This being done, we deduce that $R = T$ in the minimal case and now it's all over.

The book could have stopped here, safe in the knowledge that it had done its job, but in fact it continues for over a hundred more pages. These pages contain articles of a slightly different nature, which are not logically necessary for a proof of Fermat's Last Theorem, but are, for the main part, explanations of other results that can now be obtained as a consequence of Wiles' $R = T$ result. For example, Wiles has proved that all semi-stable elliptic curves are modular. In the fun article by Silverberg it is proved that all elliptic curves with certain prescribed torsion subgroups (for example, an elliptic curve with three points of order 2 defined over the rationals) are modular, and in the articles by Rubin and Diamond an explanation is given of the result that if an elliptic curve over the rationals is semi-stable at 3 and 5, then it is modular. (In fact, to my knowledge, the strongest statement proven so far is the recent result of Conrad, Diamond and Taylor [1], not covered in the book, which proves, amongst other things, that an elliptic curve whose conductor is not a multiple of 27 is modular.) There are articles by Lenstra–Stevenhagen and Rosen on what was known about Fermat's Last Theorem itself before the connection with elliptic curves was discovered. Finally, the last two articles, by Frey and Darmon, explain the many conjectures that are still left in the subject—for example, in Frey's article it is pointed out that Wiles has proved that for many elliptic curves E, there is a modular curve X and a map $X \to E$, but is there a good bound on the degree of this map? A strong result of this kind would be enough to imply the ABC conjecture, which still remains open despite Wiles' work. Finally Darmon humbles us by reminding us about the Birch–Swinnerton-Dyer conjecture: this conjecture, when originally formulated, said that given an elliptic curve E over the rationals, the order of a certain group which was not known to be finite should be related to the value of the L-function of E at $s = 1$, a place where it was not known to be

defined. Thanks to Wiles' work, we now know that for many elliptic curves, one side of this conjecture (the L-function side) is now known to be defined! One could argue that this was at least a good start.

5. Summary

This book offers something to a large class of readers. From the beginning graduate student, who wants to learn something about, for example, the arithmetic of elliptic curves and modular curves, to the researcher who wants to see the techniques used in Wiles' proof, to the expert who knows the techniques but wants to see their current status, there is something here. Another bonus is that various parts of the proof have been slightly simplified since the articles [7] and [6] came out, and naturally the book contains the simplified proof as opposed to the original one. It also puts into perspective that the proof ultimately really is rather long and deep, and yet has a real structure to it, namely $R = T$ in minimal case, implies $R = T$, implies semi-stable curves are modular, implies Fermat's Last Theorem. Moreover the book isolates these steps and goes into them in great detail, making it possible to concentrate on them one at a time, or indeed letting readers decide for themselves which parts they want to understand and then letting them concentrate only on these parts. Perhaps in fifty years' time there will be a much simpler proof of Fermat's Last Theorem, but at least until then we have a very fine book explaining many of the details behind the only proof that we have now.

References

[1] B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially crystalline Galois representations*, to appear in Journal of the American Mathematical Society **12** (2) (1999).
[2] G. Cornell and J. H. Silverman, *Arithmetic geometry*, Springer Verlag, 1986. MR **89b:**14029
[3] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, LNM 349, Springer-Verlag (1973), 143–316. MR **49:**2762
[4] H. Jacquet and R. Langlands, *Automorphic forms on GL_2*, LNM 114, Springer-Verlag, 1970. MR **53:**5481
[5] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Stud. 108, Princeton University (1985). MR **86i:**11024
[6] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. 141 (1995), 553–572. MR **96d:**11072
[7] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. 141 (1995), 443–551. MR **96d:**11071

Kevin Buzzard
Imperial College of Science, Technology and Medicine
E-mail address: buzzard@ic.ac.uk