Wiles Receives NAS Award in Mathematics

Andrew J. Wiles of Princeton University has received the National Academy of Sciences Award in Mathematics. Established in 1988 by the AMS in commemoration of its centennial, this $5,000 prize recognizes excellence in research in the mathematical sciences published within the last ten years. Previous recipients are Robert P. Langlands (1989) and Robert D. MacPherson (1993).

Wiles was cited for "his proof of Fermat's Last Theorem, by discovering a beautiful strategy to establish a major portion of the Shimura-Taniyama conjecture, and for his courage and technical power in bringing his idea to completion."

The Work of Andrew Wiles

The Notices *asked John H. Coates of the University of Cambridge to comment on the work of Andrew Wiles. Professor Coates supplied the following.*

After reading mathematics as an undergraduate at Merton College, Oxford, Andrew Wiles came to Clare College, Cambridge, in the academic year 1974–75 to take Part III of the Mathematical Tripos (the fourth year of the Tripos, which is roughly equivalent to the first year of graduate study in the United States). His talents were quickly noticed by Peter Swinnerton-Dyer, who, happily for me, was too busy running the University of Cambridge to be able to supervise him as a research student. Accordingly, when Andrew began research in the summer of 1975, it was my good fortune to be able to guide his first footsteps in mathematical research. I proposed to him that we work together on studying the arithmetic of elliptic curves with complex multiplication by the methods of Iwasawa theory. Our strategy was to try to establish for the fields generated by points of finite order on an elliptic curve E with complex multiplication, which is defined over the rational field $\mathbb{Q}$, precise analogues of the principal results of a celebrated paper by Iwasawa on cyclotomic fields which was published in the *Journal of the Mathematical Society of Japan* in 1964. This was essentially virgin soil, and we were eventually able to prove some parallel results to Iwasawa, showing as a corollary that if E had a rational point of infinite order, then the L-function of E must vanish at $s = 1$, as predicted by the conjecture of Birch and Swinnerton-Dyer. Andrew played at least as great a role as I in all of this work, and I quickly became conscious of his possessing two remarkable mathematical attributes, which, I believe, have played a key role throughout his subsequent mathematical career. Firstly, he wanted above all to prove hard concrete theorems, rather than formulate elegant and all-embracing conjectures. Secondly, he had an astonishing capacity to absorb large bodies of sophisticated and very abstract machinery and to bring it to bear with great effect upon down-to-earth problems. An early example of both these qualities in action was his beautiful generalization, in 1977, to arbitrary Lubin-Tate formal groups of the mysterious explicit reciprocity law of Artin-Hasse-Iwasawa for the Hilbert norm residue symbol in local cyclotomic fields.

The central problem of Iwasawa theory in the 1970s was to prove the so-called main conjecture on cyclotomic fields, and Andrew Wiles went to Harvard in September 1977 convinced that the right way of attacking this problem was via the theory of modular curves. As this shift to the study of modular curves and modular forms proved to be the decisive factor in his whole subsequent mathematical work, it is worth saying a little about the background to these ideas. Let p be an odd prime number, and let F be the field generated over $\mathbb{Q}$ by the p-th roots of unity. The origin of the main conjecture was Kummer's extraordinary work, inspired by his attempts to prove Fermat's Last Theorem, relating the p-primary subgroup of the ideal class group of F to the p-adic properties of the values of the Riemann zeta function at the odd negative integers. Iwasawa made a fundamental conceptual step forward in our understanding of Kummer's ideas in the 1960s by showing that the p-adic analogue of the Riemann zeta function, whose existence was implicit in Kummer's congruences, was not just related to the arithmetic of F but more generally to the arithmetic of the whole infinite tower of number fields obtained by adjoining all p-power roots of unity to $\mathbb{Q}$. In fact, Iwasawa was able to prove a deep theorem in this direction concerning the cyclotomic units unconditionally and posed, as an open question, a stronger statement relating the p-adic zeta function to the p-primary part of the ideal class group of this infinite tower. It was this open question which became known as the main conjecture. Iwasawa himself proved the main conjecture when the p-primary subgroup of the ideal class group of F is not too big as a Galois module (for example, if the class number of the maximal real subfield of F is prime to p), but, at the time, it seemed that one needed ideas from outside the theory of cyclotomic fields to avoid some hypothesis of this kind. Perhaps one should stress that even today, after the proof of the main conjecture, essentially nothing is known unconditionally about the precise Galois module structure of the p-primary subgroup of the ideal class group of F. The first major step towards a general proof of the main conjecture was made by Ken Ribet in a beautiful paper published in *Inventiones Mathematicae* in 1976. In this paper he used modular forms to construct the unramified p-extension of F, with given Galois action, whose existence was predicted by the main conjecture if the appropriate value of the zeta function is divisible by p. Of course, by class field theory, unramified p-extensions of F correspond to quotients of the p-primary subgroup of the ideal class group of F. Ken lectured on this work in Cambridge on several occasions as it evolved, and I believe that it was decisive in influencing Andrew Wiles to move to the study of modular forms and curves.

Andrew J. Wiles

On arriving at Harvard, Andrew Wiles set about strengthening Ribet's result by using the deep methods developed by Barry Mazur in his paper on modular curves published in the *Publications Mathematiques I.H.E.S.* in 1978. Let G be the absolute Galois group of $\mathbb{Q}$. The underlying idea of this approach was to try to find the desired unramified extensions of the field obtained by adjoining all p-power roots of unity to $\mathbb{Q}$ by studying a subquotient of the natural representation of G on the Tate module of the abelian variety associated with cusp forms of weight 2 on the subgroup of $SL_2(\mathbb{Z})$ consisting of matrices which are congruent to the identity modulo p. Technically, this was a daunting task requiring a blend of subtle techniques from the fine geometry of modular curves and their reductions and from the arithmetic of cyclotomic fields. I think it is fair to say that most mathematicians would not have had the courage to carry through such a programme, even with the benefit close at hand of Barry Mazur's knowledge of, and insight into, modular curves. But Andrew persevered, and with complete justification, as this turned out to be the beginning of an astonishingly rich vein of research, the first public account of which was given in a paper in *Inventiones Mathematicae* in 1980. Subsequently, in a joint paper full of beautiful ideas and great technical virtuosity, Mazur and Wiles in 1984 gave the first complete proof of the Iwasawa main conjecture by a development of these methods. It was natural to try to extend these modular techniques to prove the analogue of the main conjecture for the fields obtained by adjoining all p-power roots of unity to an arbitrary totally real field K, and this was the next task that Andrew set himself. This required a different approach to that of his joint paper with Mazur, as the cuspidal group, which had played such a central role in their earlier work, simply did not exist in the general totally real case. He discovered a new method (see his paper in the *Annals of Mathematics* in 1986), which again seems to have been initially inspired by Ribet's 1976 paper, based on congruences between modular forms and p-adic Galois representations attached to modular forms. The required Galois representations associated with Hilbert modular forms were not known to exist when K has even degree over $\mathbb{Q}$, and in yet another brilliant tour de force (see his article in *Inventiones Mathematicae* in 1988) he showed how one could exploit ideas of Hida about p-adic families of modular forms to construct these representations, at least in the all-important ordinary case (Richard Taylor extended his method to the general case shortly afterwards). This then enabled him to give a general proof of the main conjecture for all totally real K and all odd primes p, which was finally published in two papers in the *Annals of Mathematics* in 1990. An interesting corollary of this work, which has attracted less attention than it deserves, is that it proves the Artin conjecture about the holomorphy of the p-adic analogues of the nonabelian Artin L-functions attached to representations of the Galois groups of finite extensions of $\mathbb{Q}$. There is a final curious twist to the history of the main conjecture in the original case of cyclotomic extensions of $\mathbb{Q}$. When Kolyvagin (and in a special case, also Thaine) introduced in the late 1980s the ingenious notion of an Euler system, it immediately became likely that one could use Euler systems to complete Iwasawa's original approach to proving the main conjecture. Such a proof was given shortly afterwards by Karl Rubin (who also carried through, by analogous but more difficult techniques, the proof of the main conjecture for elliptic curves with complex multiplication which grew out of Wiles's and my original work), and so one can argue that today we have a proof of the main conjecture using only abelian class field theory and ideas about cyclotomic fields which, at least in principle, were known to Kummer. However, the modular techniques developed by Andrew Wiles are not only of great interest in their own right, but are indispensable in handling the totally real case, since it is highly unlikely that anyone will ever succeed in proving the existence of good analogues of cyclotomic units and Euler systems for totally real fields which are not abelian over $\mathbb{Q}$.

These contributions to the study of both the main conjecture of Iwasawa theory and Galois representations attached to Hilbert modular forms had already placed Andrew Wiles amongst the select few over the last 150 years who have made profound contributions to algebraic number theory. However, as we now know, he did not rest on these laurels, and since the summer of 1986 he was quietly working towards a greater goal. The story of his revolutionary work proving that every semistable elliptic curve over $\mathbb{Q}$ is modular, with its corollary that Fermat's Last Theorem is finally proven, is perhaps better known and more fully documented than any event in the whole history of mathematics. Andrew himself has given a rather detailed account of how this research evolved in the introduction to his great paper on modular elliptic curves and Fermat's Last Theorem published in the *Annals of Mathematics* in 1995, and it seems pointless for me to even attempt a summary here. While it has always been true that Fermat's Last Theorem has excited strong passions amongst both amateur and professional mathematicians alike, one can nevertheless legitimately ask why this piece of mathematics has generated such unprecedented interest. I think that, for the working algebraic number theorist, the answer is fairly clear, especially if one looks at the evolution of the subject over the last 35 years. On the one hand, there is the sheer conceptual beauty of the proof, which brings decisively together so many of the different strands of research developed on the arithmetic modular forms and the number-theoretic interpretation of the special values of L-functions (I shall not even attempt here to list all mathematicians whose work contributed to the final solution beyond citing the obvious names of Flach, Frey, Langlands, Mazur, Ribet, and Taylor). On the other hand, it is probably no exaggeration to say that much of algebraic number theory and arithmetical algebraic geometry over the last 35 years has been dominated by conjectures rather than decisive theorems. This is meant in no way to denigrate the many beautiful theorems which have been proven during this time, but simply to point out that so often these positive results have seemed modest when placed against the vast array of overlapping conjectures whose proof remains the long-term goal of algebraic number theory (for example, the conjecture of Birch and Swinnerton-Dyer on the arithmetic of elliptic curves, or Artin's conjecture on the holomorphy of his non-abelian L-functions). Andrew Wiles's work has been a wonderful antidote to this pattern of research and is the most striking reminder in our times that we can eventually hope to find proofs of the deepest mysteries in number theory. The National Academy of Sciences is to be congratulated for selecting him as their 1996 prizewinner.

John Coates

Biographical Sketch

Andrew J. Wiles was born in Cambridge, England, on April 11, 1953. He attended Merton College, Oxford University, starting in 1971, and he received his B.A. there in 1974. That same year he went to Clare College, Cambridge University, earning his Ph.D. there in 1980.

From 1977 until 1980, Wiles was a Junior Research Fellow at Clare College and a Benjamin Peirce Assistant Professor at Harvard University. In 1981 he was a visiting professor at the Sonderforschungsbereich Theoretische Mathematik in Bonn, and later that year he was a member of the Institute for Advanced Study in Princeton. In 1982 he became a professor at Princeton University and in the spring of that year was a visiting professor at the University of Paris, Orsay. On a Guggenheim Fellowship he was a visiting professor at the Institut des Hautes Études Scientifiques and at the École Normale Supérieure (1985–1986). From 1988 to 1990 he was a Royal Society Research Professor at Oxford University. In 1994 he assumed his present position as Eugene Higgins Professor of Mathematics at Princeton.

Wiles was elected a Fellow of the Royal Society, London, in 1989. In 1995 he received the Schock Prize in Mathematics from the Royal Swedish Academy of Sciences. That same year he was awarded the Prix Fermat, presented by the Université Paul Sabatier and Matra Marconi Space. In 1996 Wiles received the Wolf Prize in mathematics.