MAPLE TECH

MAPLE IN MATHEMATICS AND THE SCIENCES

SPECIAL ISSUE
1994

The Status of Fermat's Last Theorem – mid 1994

Andrew Granville and Michael Monagan[1]

On Tuesday October 25th, 1994, after this article was written, the following two manuscripts were released:

- *Modular Elliptic Curves and Fermat's Last Theorem*, by Andrew Wiles
- *Ring Theoretic Properties of Certain Hecke Algebras*, by Richard Taylor and Andrew Wiles

The first one (long) announces a proof of, among other things, Fermat's Last Theorem, relying on the second one (short) for one crucial step, thus repairing the gap in Wiles' previous attempted proof.

In the words of my co-author, "I think we can believe that it is done now."

Introduction

Given all the recent excitement over Wiles' important attack on Fermat's Last Theorem (as well as the far more general Taniyama Conjecture), it seems appropriate to review what Wiles has done, where that leaves the study of Fermat's Last Theorem, and what role Maple has played in research on this subject. In this news article, we outline the direction of Wiles' work and then survey other developments in the field. But first, what is Fermat's Last Theorem, and why is it still so intriguing?

Fermat's Last Theorem

Pierre-Simon de Fermat (1601–1665) a jurist by profession from Toulouse, studied mathematics as a hobby. He didn't formally publish his work but rather disseminated his ideas in letters, challenging others to match and/or admire his understanding. Fermat was evidently inspired by Diophantus' *Arithmetic*[2] and made many notes in the margin of his copy. After Fermat's death, his son Samuel published these notes and amongst them was the following tantalizing sentence, beside the description of Pythagoras' Theorem:

> "...it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

Stated mathematically, one cannot find whole numbers a, b, c, and n, with n bigger than 2, for which

$$a^n + b^n = c^n.$$

Whether Fermat was being overly optimistic about his 'demonstration', we shall probably never know, but his argument has not been reproduced in the intervening three and a half centuries, despite no shortage of effort to do so. Ernst Kummer, the German mathematician of the last century who did so much to establish modern algebra, wrote that Fermat's Last Theorem is "more of a joke than a pinnacle of science", yet his own most important work originated in failed attempts to prove it! The problem has become perhaps the most famous one in mathematics. A lot of mathematics has been invented as a result of attempts to prove Fermat's Last Theorem. The interested reader is recommended to read Ribenboim's "13 Lectures on Fermat's Last Theorem." (See [16] for an introduction to the subject.)

To begin with, let us note that in order to prove Fermat's Last Theorem, we need only consider exponents n which are odd primes. This is because if we have a solution $a^{pq} + b^{pq} = c^{pq}$ with exponent pq, then we have a solution $(a^q)^p + (b^q)^p = (c^q)^p$ for exponent p (note that any integer > 2 either has an odd prime factor p or is divisible by 4).

The Taniyama Conjecture

Our story begins in 1955 when Taniyama conjectured the most extraordinary connection between modular forms and elliptic

[1]Institute for Scientific Computing, ETH Zurich, CH-8092 Zurich, Switzerland, monagan@inf.ethz.ch

[2]One of the great intellectual masterpieces of the ancient Greek world. This work, available in the seventeenth century in Latin translation, was an important inspiration for the scientific renaissance of that period, read by Fermat, Descartes, Newton, and others.

curves. Authors have written complicated, lengthy articles trying to describe precisely what this conjecture is, and so rather than going into a technical description we will instead just give the flavor of Taniyama's Conjecture by selecting one classical example. For our purposes, an *elliptic curve* will be the real points on the curve

$$y^2 = x^3 + ax + b$$

for selected values of a and b. In particular, we want to study rationals x, y, and values of x and y modulo p, that satisfy this equation. Gauss considered the solutions x, y with $1 \leq x$ and $y \leq p$ to the equation $y^2 \equiv x^3 - x \pmod{p}$. If you check this out with a Maple program, you will quickly discover that the number of such points is exactly equal to p for $p = 2$ or for any prime $p \equiv 3 \pmod{4}$. For primes congruent to 1 mod 4, it is a little more mysterious. You might like to build your own table of values and see if you can guess the solution. We constructed the following table using Maple (where $n(p)$ counts the number of solutions):

p	$n(p)$	$a(p)$
5	7	−1
13	7	3
17	15	1
29	39	−5
37	39	−1
41	31	5
53	39	7
61	71	−5

You can see that the numbers $n(p)$ are all close to p and in fact they are all odd. It thus makes sense to consider $a(p) = \frac{p-n(p)}{2}$. What are these new numbers $a(p)$? They all seem to be odd and small. Take a moment and try to guess.

What Gauss realized was that the $a(p)$ are determined by a famous special property of primes congruent to 1 mod 4, which, incidentally, was discovered by Fermat. That is, that they can be written in a unique way as a sum of two squares. Let's try it with these primes. We have $5 = 1^2 + 2^2$, $13 = 3^2 + 2^2$, $17 = 1^2 + 4^2$, $29 = 5^2 + 2^2$, $37 = 1^2 + 6^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$, and $61 = 5^2 + 6^2$.

Now can you guess what the numbers $a(p)$ are above? As you can see, if you write $p = a^2 + b^2$ with a odd and b even, then $a(p) = \pm a$. With a little more work you can probably guess what the sign is. In fact, $a(p) = (-1)^{\frac{a+b-1}{2}} a$. What a beautiful fact! What we have observed is that

$$\begin{aligned} n(p) &= p - 2(-1)^{\frac{a+b-1}{2}} a \\ &= p - \sum_{\substack{p=a^2+b^2 \\ a \text{ odd},\ b \text{ even}}} (-1)^{\frac{a-1}{2}} a \cdot 2(-1)^{\frac{b}{2}}, \end{aligned}$$

a fact that vacuously holds true for primes $p \equiv 3 \pmod{4}$, and for $p = 2$.

What on earth does all this have to do with the mysterious subject of modular forms? Adequately describing a modular form is an arduous task (though beautiful — see [12]) so instead we'll discuss the "predecessors" to modular forms, the beautiful identities of Jacobi (see [12], sections 19.8,9). Jacobi's triple product identity states that

$$q \prod_{n \geq 1} (1 - q^{8n})^3 = \sum_{a \text{ odd}, \geq 1} (-1)^{\frac{a-1}{2}} a q^{a^2}.$$

Expanding the left-hand side as a truncated power series in Maple, we can check this identity for the first few terms.

```
> series(q*product((1-q^(8*n))^3,n=1..10),
>     q=0,80);
```

$$q - 3q^9 + 5q^{25} - 7q^{49} + O\left(q^{81}\right)$$

Another famous identity of Jacobi (that you should also verify with Maple) is

$$\prod_{n \geq 1} \frac{(1 - q^{4n})^2}{(1 - q^{8n})} = 1 + 2 \sum_{b \text{ even}, \geq 2} (-1)^{\frac{b}{2}} q^{b^2}.$$

Can you see what these two marvelous identities have to do with $n(p)$? By multiplying them together we find that $q\left(\prod_{n\geq 1}(1-q^{4n})(1-q^{8n})\right)^2$ equals

$$\sum_{a \text{ odd} \geq 1} (-1)^{\frac{a-1}{2}} a q^{a^2} + \sum_{\substack{a \text{ odd} \geq 1 \\ b \text{ even} \geq 2}} (-1)^{\frac{a-1}{2}} a \cdot 2(-1)^{\frac{b}{2}} q^{a^2+b^2}.$$

We see that the coefficient of q^p is given by $(-1)^{\frac{a-1}{2}} a \cdot 2(-1)^{\frac{b}{2}}$, summed over all solutions to $p = a^2 + b^2$ with a odd and b even; which is exactly the difference between p and $n(p)$. Could this be a coincidence? Could these strange identities have anything to do with counting points modulo p on an elliptic curve? Well, Taniyama's Conjecture is that it not only is *not* a coincidence, but in fact that, for every elliptic curve, you can find a power series, not unlike

$$q\left(\prod_{n\geq 1}(1-q^{4n})(1-q^{8n})\right)^2,$$

(in fact, a modular form) such that, for all but finitely many primes p, the coefficient of q^p equals p minus the number of points on the elliptic curve modulo p. Before Wiles' work, this was only known for some very special elliptic curves (the so-called "CM curves", as proved by Shimura), which have a lot in common with the example we have just discussed.

The Connection to Fermat's Last Theorem

The recent, extraordinary breakthrough for Fermat's Last Theorem stems from an important observation made by

Gerhard Frey in 1986. What he observed was that given any solution to Fermat's equation $a^p + b^p = c^p$, we could study the elliptic curve $y^2 = x(x - a^p)(x + b^p)$. This curve has the strange property that the differences of the pairs of roots of $x(x - a^p)(x + b^p)$ are a^p, b^p, and c^p, that is, they are each pth powers. If we assume that the Taniyama Conjecture is true for this elliptic curve, then the associated power series (modular form) in q would have to have the most amazing properties, and Frey proposed that no such power series could possibly exist. Following an idea due to Serre, Ken Ribet was able to prove that there cannot be such a power series (that is, a modular form corresponding in the appropriate way to the elliptic curve $y^2 = x(x - a^p)(x + b^p)$). In other words, Ribet proved that Fermat's Last Theorem follows from the truth of Taniyama's Conjecture.

Andrew Wiles' Work

In the summer of 1993, Andrew Wiles claimed to have proved Taniyama's Conjecture for a large class of elliptic curves, including those relevant to Fermat's Last Theorem. His proof is an extraordinary synthesis of the latest techniques in many areas of mathematics and it is said that if written down to be accessible to most mathematicians, it would cover over one thousand pages. The latest situation, as of August 1994, is that there are some problems with part of the proof; in particular with an upper bound on the order of the relevant *Selmer group*. It is not clear at this time whether his proof is completely recoverable. However, he *has* indisputably proved the Taniyama Conjecture for a very wide class of elliptic curves (in particular an infinite sequence of curves with distinct 'j-invariants', that is the number $4a^3/(4a^3 + 27b^2)$). This alone amounts to a great breakthrough in one of the central questions of number theory. This summer, in his plenary lecture at the International Congress of Mathematicians in Zurich, Wiles clearly explained what remains to be proved and outlined his plausible line of attack; we can only hope that in the not-too-distant future the proof of Fermat's Last Theorem will be completed.

Other Work

In the meantime, we will review other recent results on Fermat's Last Theorem, some of which have been proven with the use of Maple. One of the greatest works of algebra was Kummer's celebrated attack on Fermat's Last Theorem in the mid 19th century. Kummer was able to prove Fermat's Last Theorem for the so-called *regular* primes, that is, primes p such that p does not divide the numerator of B_{2n}, the $2n^{th}$ Bernoulli number, for any n in the range $2 \le 2n \le p - 3$. This hypothesis has been weakened to allow Buhler, Crandall, and Sompolski to prove Fermat's Last Theorem for all exponents p up to 4 million in 1992.

In 1983, Gerd Faltings proved that there are only finitely many rational solutions x, y to any algebraic equation of the form $f(x, y) = 0$, except in certain cases which can be explicitly described (for example, if f is of degree one, and often if f is of degree two or three). In particular, a solution of $a^p + b^p = c^p$ yields a solution to $x^p + y^p = 1$, with $x = a/c$ and $y = b/c$. Applying Faltings' theorem to this latter equation we see that there are only finitely many solutions to Fermat's Last Theorem for any fixed exponent p. Faltings won the 1986 Fields' Medal (the "Nobel Prize of mathematics") for this work. In 1985 Granville and Heath-Brown used Faltings' theorem to show that Fermat's Last Theorem holds for "almost all" exponents.

It is traditional to split Fermat's Last Theorem into two cases: the first case (FLT1) where the prime exponent p does not divide abc; and the second case (FLT2) where p does divide abc. The first case turns out to be much easier to attack. In 1985, developing ideas of Sophie Germain from the early eighteenth century, Adleman, Fouvry, and Heath-Brown showed that FLT1 holds for infinitely many different prime exponents p.

Kummer's methods (referred to above) can be modified to obtain extraordinary consequences if there is a solution to FLT1. For example, p would not only be irregular but, in fact, p divides B_{2n} for more than $\sqrt{p}$ values of n in the range $2 \le 2n \le p - 3$. Recently McCallum went much further, showing that if there are at least $2(p - 1)$ different solutions to $a^p + b^p = c^p$ where p does not divide abc, then p divides more than $p/8$ such Bernoulli numbers.

In 1909 Wieferich showed that if FLT1 is false for prime exponent p, then p^2 divides $2^p - 2$. Using a computer, Lehmer in 1981 checked this for all primes $p < 6 \times 10^9$ and found it false except for $p = 1093$ and $p = 3511$. (Crandall and Dilcher are currently pushing this value up a lot higher.)

Numerous mathematicians, such as Frobenius and Pollaczek, have generalized Wieferich's result (i.e., p^2 divides $3^p - 3$, $5^p - 5$, etc.) so that more primes can be ruled out. In 1988 Granville and Monagan obtained:

> If FLT1 is false for prime exponent p, then p^2 divides $q^p - q$ for each prime $q \le 89$.

Part of the proof involved numerous computations which were done in Maple. The computations which proved to be the most difficult were computing determinants of matrices (of dimension up to 43) of univariate polynomials (of degree up to 50) with small integer coefficients, computing resultants of these polynomials (of degree up to 464), computing the Hermite normal form of integer matrices (of dimension up to 54), and factoring some large integers (up to 153 digits in length).

length). Note, the most difficult integer factorizations were done with the help of other systems.

Coppersmith has used our result to prove that FLT1 holds for all prime exponents up to 7.56×10^{17}. In unpublished work, Suzuki extended the above to all $q \leq 103$ using a Hitachi super computer, which presumably will lead to a larger bound.

Recently, Skula proved that a solution to FLT1 implies there are many rational roots $\frac{a}{q}$ to $B_{p-1}(\frac{a}{q}) \equiv 0 \pmod{p}$. Using Maple, Cikánek, Dilcher, and Skula proved this for $1 \leq a \leq q \leq 89$.

A quite different consequence to a solution to FLT1 for exponent p was recently found by the Sun brothers: It is well-known that if F_n is the nth Fibonacci number then prime p must divide $F_{p-(5/p)}$ where $(5/p) = 1$ if $p \equiv \pm 1 \pmod{5}$, $(5/p) = -1$ if $p \equiv \pm 2 \pmod{5}$, and equals 0 if $p = 5$. However, there is no prime known for which p^2 divides $F_{p-(5/p)}$, and this has now been checked for all primes $p \leq 100,000$. However, the Suns proved that if there is a solution to FLT1 for exponent p, then p^2 must divide $F_{p-(5/p)}$.

Short proofs of most of the results stated in this section may be found in [?].

Fermat's Last Theorem is currently a living, vibrant area of research. Besides Wiles' work, there are also significant new ideas from Kolyvagin, McCallum, and Thaine from deep arithmetic geometry. Researchers like Skúla, Agoh, Dilcher, and Jha are bringing new ideas from an algebraic number theory perspective. It is evident in many of these papers that some of the ideas were developed first through studying the data from explicit computations (yes, often done in Maple), and only then proceeding to a formal proof. We look forward to seeing further important developments in the subject, both theoretical and computational.

References

[1] L.M. Adleman and D.R. Heath-Brown, The first case of Fermat's Last Theorem, *Invent. Math.*, **79**, pp. 409–416, (1985).

[2] J.P. Buhler, R.E. Crandall and R.W. Sompolski, Irregular primes to one million, *Math. Comp.*, **59**, pp. 717–722, (1992).

[3] P. Cikánek, Special extension of Wieferich criterion, *Math. Comp.*, **62**, pp. 923–930, (1994).

[4] D. Coppersmith, Fermat's Last Theorem (case 1) and the Wieferich Criterion, *Math. Comp.*, **54**, pp. 895–902, (1990).

[5] K. Dilcher and L. Skula, A new criterion for the first case of Fermat's Last Theorem, *Math. Comp.*, to appear.

[6] G. Faltings, Endlichkeitssätze für Abelsche Varietaten Zahlkorpern, *Invent. Math.*, **73**, pp. 349–366, (1983).

[7] E. Fouvry, Théorème de Brun-Titchmarsh. Application au théorème de Fermat, *Invent. Math.*, **79**, pp. 383–407, (1985).

[8] G. Frey, Links between solutions of $A - B = C$ and elliptic curves, *Lecture Notes in Mathematics*, **1380**, pp. 31–62, (1987).

[9] A. Granville, The set of exponents for which Fermat's Last Theorem is true, has density one, *C.R. Acad. Sci. Canada*, **7**, pp. 55–60, (1985).

[10] A. Granville, On the Kummer-Wieferich-Skula criteria for the first case of Fermat's Last Theorem, in *Advances in Number Theory* (ed. F.Q. Gouvea and N. Yui), Oxford, New York, pp. 479–498, (1993).

[11] A. Granville and M. B. Monagan, The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389, *Trans. American Math. Soc.*, **306**, pp. 329–359, (1988).

[12] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford, Clarendon, (1979).

[13] D.R. Heath-Brown, Fermat's Last Theorem true for almost all exponents, *Bull. London Math. Soc.*, **17**, pp. 15–16, (1985).

[14] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, *Graduate Texts in Mathematics*, **97**, Springer-Verlag, New York, (1993).

[15] W.G. McCallum, The arithmetic of Fermat curves, *Math. Ann.*, **294**, pp. 503–511, (1992).

[16] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, (1979).

[17] K. Ribet, On modular representations of $Gal(\overline{Q}/Q)$ arising from modular forms, *Invent. Math.*, **100**, pp. 431–476, (1990).

[18] L. Skula, Fermat's Last Theorem and the Fermat quotients, *Comm. Math. Univ. Sancti Pauli*, **41**, pp. 35–54, (1992).

[19] Z.-H. Sun and Z.-W. Sun, Fibonacci numbers and Fermat's Last Theorem, *Acta Arithm.*, **60**, pp. 371–388, (1992).

[20] Thaine, F., On the ideal class groups of real abelian number fields, *Annals of Math.*, **128** pp. 1–18, (1988).