Fermat's Last Theorem

[To appear in Enciclopedia Italiana, Appendice 2000]

Introduction. Fermat's Last Theorem surely was mathematics' most celebrated and notorious open problem. Its investigation sparked fundamental advances in the mathematical sciences.

Fermat's Last Theorem states that there are no positive integer x, y and z so that

$$x^n + y^n = z^n$$

if n is an integer greater than 2.

For $n = 2$ there is an infinity of solutions

$$3^2 + 4^2 = 5^2, 5^2 + 12^2 = 13^2, 8^2 + 15^2 = 17^2, \ldots$$

the Pythagorean triples. However, in 1637 or so, the French jurist Pierre de Fermat wrote in the margin of his copy of the *Arithmetica* of Diophantus, at problem 8 in Book II, at which it is asked to split a square into squares that, on the other hand:

> *Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

That is: "To split a cube into two cubes, or a fourth (biquadratic) power into two fourth powers, or indeed any higher power unto infinity into two like powers, is impossible; and I have a marvellous proof for this. But the margin is too narrow to contain it."

On Fermat's death in 1665 his son Samuel proceeded to collect Fermat's mathematical correspondence. That, and a reprint of the *Diophantus*, together with Fermat's marginal notes, was published in 1670. By the end of the eighteenth century all of Fermat's other remarks had been dealt with, one way or the other: either properly proved or shown to be false. Only this one remark, hence the *last* theorem, remained.

When Fermat died in 1665 he was one of the most famous mathematicians in Europe. But he did not publish. His reputation grew out of his correspondence with other scholars and out of a number of works which circulated in manuscript form. Incidentally, it's quite absurd to suppose that Fermat had a proof of the 'Last Theorem'. Indeed, it seems plain that he did not continue to believe that he had one much beyond the moment he scribbled the claim in that notorious margin. Other than for the exponents 3, and 4, which were within his reach and which are mentioned as challenge problems in his letters, Fermat never boasted about the matter in his correspondence in the thirty or so remaining years of his life.

Nowadays, one thinks of Fermat principally as a number theorist. But at the time his work in number theory was so revolutionary and so much ahead of its time that its value was poorly understood. His work then most celebrated included

his contributions to optics, particularly his principle of least time and thus the law of reflection; to analytic geometry (which he had developed independent of Descartes); and his theory of tangents, quadrature, and of maxima and minima — the beginning of calculus. Those contributions are now mostly forgotten, perhaps because they were just the first steps in matters now much better understood. On the other hand, Fermat's work in number theory, as interpreted a century and more later by Euler and subsequent originators of modern mathematics, remains fresh and inspiring.

To prove Fermat's Last Theorem one need only show that no fourth power is a sum of two fourth powers, and — for all odd primes p — no p-th power is a sum of two p-th powers. That these cases suffice is clear, because any integer $n \neq 2$ is either a power of two, and so divisible by 4, or n is divisible by some odd prime p. So an n-th power (other than a square) plainly is also either a fourth power, or it is also a p-th power for some odd prime p.

In one of the few actual proofs he left behind, Fermat himself had dealt with case $n = 4$. Specifically, Fermat shows that a right-angled triangle with integer sides cannot have area the square of an integer. One recalls that primitive Pythagorean triples $x^2 + y^2 = z^2$ are all of the shape $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$ for coprime integers u and v not both odd. It's then an interesting, and not quite a trivial, exercise to notice that the nonexistence of the right-angled triangle entails that a difference of two fourth powers cannot even be a square, let alone a fourth power.

It was a century later, in 1753, that Euler dealt with the case $n = 3$. There was an apparent omission in the argument, later filled in by Gauss. Dirichlet and Legendre proved the case $n = 5$ in 1825 and Lamé settled the case $n = 7$ in 1839; Dirichlet had proved the case $n = 14$ in 1832.

The first and second cases. From here on p is an odd prime. For symmetry, it is often convenient — as one may, say, by taking c negative — to consider Fermat's equation in the form $a^p + b^p + c^p = 0$, where, of course, we may suppose that a, b, c do not share a common factor; so no two have a common factor. One then readily sees that there are two cases, according as the exponent p divides one of a, b, or c — say, c; or as not. In the latter case, the First Case of FLT, it's then easy to show that there is an integer γ so that $a + b = \gamma^p$. On the other hand, if c is divisible by p, thus the Second Case, then $a + b = p^{p-1}\gamma^p$.

Sophie Germain, used these ideas to show that there is no First Case solution if both the exponent n, and $kn + 1$, are primes; here k may take various small values. It followed from her work as generalised by Legendre that Fermat's equation has no First Case solution for exponent n less than 100.

Much more recently, Adleman and Heath-Brown applied a result of Fouvry to generalise Sophie Germain's ideas so as to prove that the First Case of Fermat's Last Theorem holds for infinitely many prime exponents.

Abel had conjectured that none of x, y or z can be a power of a prime. Using formulas such as those alluded to above one can show that if in $x^n + y^n = z^n$, with $0 < x < y < z$ and $n \geq 3$, one of x, y or z is some power q^r of a prime q, then

the exponent n must be some prime p, the prime power must be $x = q$, z differs from y by 1, and n divides $y(y+1)$. However, until the recent proof of Fermat's Theorem in general it was not even known that 'Abel's equation' $x^p + y^p = (y+1)^p$ is impossible in positive integers x and y.

The Barlow–Abel formulæ, as the formulas above may be called, are often rediscovered. Particularly if the equations are manipulated in their non-symmetric form, it's dreadfully easy to make a minor error and thus to obtain a spurious contradiction 'proving' that Fermat's equation indeed has no integer solutions. It's frightening to contemplate the near innumerable hours spent by 'discoverers' in pursuing such dead ends, and irritating to recall the time spent in finding such errors and explaining to reluctant 'provers' that their approach always was hopeless. Sadly, Wiles' successful argument has not yet dissuaded these workers from attempting to discover an 'elementary argument' — thus one not involving any nontrivial mathematics.

Nonetheless, it was not until the seventies that Terjanian remarked, using only these elementary methods, that if $x^{2p} + y^{2p} = z^{2p}$ has a solution in integers then $2p$ divides one of x or y.

Kummer's work. Fermat's Last Theorem concerns rational integer solutions to an equation. Yet one seems to simplify study of Fermat's equation by introducing generalised integers — the so-called *cyclotomic integers* involving p-th roots of unity. The idea is to see that $x^p + y^p = z^p$ is $\prod_{r=0}^{p-1}(x + \zeta_p^r y) = z^p$, where ζ_p is a primitive p-th root of unity. One would like to be able to argue that this means that each linear factor $(x + \zeta_p^r y)$ is essentially a p-th power, as would be the case were we still dealing with rational integers. However, Kummer saw that in general there is no unique factorisation in domains of cyclotomic integers and, worse, there are nontrivial units. Kummer attacked those difficulties by introducing the notion of ideal numbers. Then the principal ideals $(x + \zeta_p^r y)$ each are p-th powers of ideals of the p-th cyclotomic field, indeed p-th powers of principal ideals if the class number of that field is prime to p. Kummer proved Fermat's Last Theorem for such *regular* primes in 1847. His researches provided a seemingly straightforward characterisation of regularity in terms of the behaviour of the Bernoulli numbers mod p, his study of cyclotomic number fields initiated the subject now known as algebraic number theory, and by dealing with the primes 37, 59 and 67, which are only 'a little irregular', Kummer proved Fermat's Last Theorem beyond exponent 100 (up to 167, where the calculations became just too burdensome).

In 1850 the Académie des Sciences de Paris offered a golden medal and a prize of 3000 francs to the mathematician who would solve Fermat's problem. In 1856 it determined to withdraw the question from competition but to award the medal to Kummer "for his beautiful researches on the complex numbers composed of roots of unity and integers".

Nonetheless, just as Gauss had dismissed Fermat's equation as one of a multitude of such diophantine equations, so Kummer made it clear that he valued his work on the higher reciprocity laws far more than its eventual application to Fermat's Last Theorem.

Until recently. The next 120 years see surprisingly little fundamental advance on Kummer's contributions to Fermat's Last Theorem. Earlier this century the United States mathematician Vandiver corrected part of Kummer's work and refined his criteria for irregularity. By 1993, further such refinements and ingenious computation had settled Fermat's Last Theorem for exponents up to four million.

At the turn of the century, work relying on a complicated analysis of Kummer's conditions led to the Wieferich criterion that if there is to be a First Case solution for exponent p, then p must divide the *Fermat quotients* $(a^p - a)/p$ both for base $a = 2$ and $a = 3$. But we now know, again by computer check, that the only primes up to 10^9, say, satisfying the criterion for $a = 2$ are 1093 and 3511, whilst for base 3 there are just 11 and 1006002. By 1993, Granville had proved the First Case criterion to be necessary for all bases up to $a = 89$, settling the First Case of Fermat's Last Theorem beyond exponent 10^{14}.

By also applying techniques from transcendence theory and diophantine approximation, the Finnish mathematician Inkeri had shown that a putative solution in the case of exponent p would have x, say, larger than p^p, or so. Thus it was known that one could not possibly actually state any counterexample to Fermat's claim, for if there were one it would involve integers millions of digits long. In that spirit, application of Baker's method showed that in $x^p + y^p = z^p$, with $0 < x < y < z$, in any case $y - x$ is nearly as large as x, and $z - y$ is either similarly large, or $z - y = 1$. So these highly sophisticated methods could not even settle Abel's conjecture.

Catalan's Conjecture, whereby the equation $x^u - y^v = 1$ has $3^2 - 2^3 = 1$ as its only nontrivial solution in integers, had been supposed more difficult than Fermat's Last Theorem. Yet, in the mid-seventies, Tijdeman refined Baker's inequalities and showed they imply that Catalan's equation has at most finitely many solutions. More recent improvements in the numerical Baker bounds and applications inter alia of class field theoretic results of Inkeri have by now considerably narrowed the range in which further solutions might occur.

In 1983 Faltings proved Mordell's Conjecture to the effect that a curve of genus greater than 1 has at most finitely many rational points. This fundamental advance in arithmetic geometry implies that each Fermat equation has at most finitely many solutions, because an integer solution to the Fermat equation provides a rational point on the curve $x^p + y^p = 1$ (here we've replaced x/z by x, and y/z by y). For $p > 3$ those curves have genus more than one. It's a simple application to show that Fermat's Last Theorem holds for almost all exponents n; that is, that the probability of any given exponent providing a counterexample is zero.

In 1908 the Königliche Gesellschaft der Wissenschaften in Göttingen had announced the Wolfskehl Prize, providing 100 000 Reichsmark "to be given to the person who will be first to prove the Great Theorem of Fermat". The adjective 'great' contrasts the result with the far more important 'Fermat's Little Theorem' according to which a prime p divides $a^p - a$ for all integers a. The 'little theorem' is fundamental to modern public key cryptography.

The Wolfskehl Prize provoked a flood of purported proofs, and rumours of its value, notwithstanding that having been grossly depleted by hyperinflation, undoubtedly remained responsible for the notoriety of Fermat's Last Theorem. To the despair

of amateurs, Andrew Wiles has now been formally awarded the Wolfskehl Prize, now again worth some 50 000DM, for his proof.

However, as already said, in the 120 years following Kummer's monumental contribution, there was little fundamental advance on that work. In particular, it can still not be proved that there are infinitely many regular primes — though one safely conjectures that a little more than 70% of primes are regular, and it's easy to prove that there are infinitely many irregular primes. It was still not known whether the Second Case of Fermat's Last Theorem holds for infinitely many prime exponents. It seemed that a quite new idea was needed. The new idea came from a seemingly quite different area of mathematics.

Recently . . . . Number theory was strong in antiquity. But the books of Diophantus were lost in the burning of the library of Alexandria and had little influence on mathematics until the seventeenth century, when Fermat was inspired by Bachet's then recent translation. The ideas underlying the solutions to the problems in the *Arithmetica* were substantially in advance of those then current in the West.

Diophantus is largely concerned with the problem of finding a rational solution to various equations; we now recognise his methods as geometrical. Dealing with the Pythagorean triples, he considers the equation $x^2 + y^2 = 1$ in rationals x and y; which we well know to be a circle. An obvious, albeit trivial, point on this locus is $(-1, 0)$. A typical line through that point is parametrised by $x = u - 1$, $y = tu$. This line intersects the circle when $u^2 - 2u + 1 + t^2u^2 = 1$; and happily we can cancel the known solution $u = 0$ to obtain $u = 2/(1 + t^2)$, yielding a new point $x = (1 - t^2)/(1 + t^2)$, $y = 2t/(1 + t^2)$. This is of course essentially the solution already mentioned above, now illustrating that the circle may be parametrised by rational functions. In this case we get infinitely many solutions, given by a simple formula. Different problems might have infinitely many solutions not given by a rational formula, or just finitely many solutions, or none at all.

Problem 24 of Book IV of Diophantus suggests that we split a given number, say 6, into two parts so that their product is a cube minus its cube root. That is, $y(6 - y) = x^3 - x$. Once again, $(-1, 0)$ provides a trivial solution but now when we try $x = u - 1$, $y = tu$ we get, after cancelling the known solution $u = 0$,

$$t(6 - tu) = (u - 1)(u - 2) \quad \text{or} \quad u^2 - (3 - t^2)u + (2 - 6t) = 0\,.$$

In general, this leads to irrational values for u. However, on selecting the slope $t = \frac{1}{3}$, we may cancel once more to obtain $u = \frac{26}{9}$ whence $x = \frac{17}{9}$, $y = \frac{26}{27}$ is a new solution. The fun thing is that we can now construct the tangent at this new solution to find a further solution, and so on. In general, given two solutions, the secant yields a third solution. Of course the complexity of the solutions threatens to increase dramatically.

For example, writing in 1643, Fermat asks for right-angled triangles so that both the hypotenuse and the sum of the two sides are squares. Taking the sides as $\frac{1}{2}(1 \pm y)$ and the hypotenuse as x^2, we of course have $y^2 = 2x^4 - 1$ by Pythagoras. Fermat can compute the basic solution $P(13, 239)$. But the geometrical problem requires that the sides of a triangle be positive numbers, so $-1 < y < 1$. The tangent at P

provides a further solution $2P\left(\frac{1525}{1343}, \frac{2750257}{1803649}\right)$. This still won't do. Finally, we get $3P\left(\frac{2165017}{2372159}, \frac{3503833734241}{5627138321281}\right)$ from the secant through two solutions, corresponding to a triangle with sides:

$$a = 1061652293520\,, \quad b = 4565486027761\,, \quad c = 4687298610289\,.$$

Not only is this a solution, but the method guarantees that this is the *smallest* solution!

With yet higher-degree equations these methods fail in general. The upshot is that given a polynomial equation $f(x, y) = 0$ with integer coefficients, there are three cases, seemingly depending on the (total) degree of f. Namely, if f is of degree at most two, we have none or infinitely many solutions — these cases are parametrised by rational functions. This is the case of *rational curves* — curves of genus 0. If f is of degree 3 we may have finitely many — the method of *infinite ascent* of the last examples may cycle, or infinitely many solutions. This is the case of *elliptic curves*; that is, curves of genus 1. These curves do not, of course have anything to do with ellipses — those are conics and may be parametrised by rational functions. Rather, the point is that these curves are parametrised by the so-called elliptic functions. Finally, there are curves of *general type*, of genus $g \geq 2$, which seem only to have sporadic rational points, thus Mordell's Conjecture ultimately proved by Faltings.

In summary, the interesting case — where it's not clear whether a curve has infinitely many rational points or not — is the case of elliptic curves. In this sense the study of the collection of equations comprising Fermat's Last Theorem is of no interest at all.

Our understanding of the arithmetic of elliptic curves had advanced remarkably in the past 50 or so years. Computation and analogy with known results for algebraic number fields had motivated the remarkable conjectures of Birch and Swinnerton-Dyer, and work of Eichler and of Shimura had given body to a suggestion of Taniyama to the effect that elliptic curves defined over the rationals are also parametrised by modular functions. Some instances of the Birch–Swinnerton-Dyer Conjectures had been proved, the simplest case established by Coates and Wiles.

Then, in the mid-eighties, there came a remarkable connection between this fundamental work and Fermat's Last Theorem. The context of that relationship arose in part from a study of the so-called ABC–conjecture according to which an equation $A + B = C$ in positive integers A, B and C entails that C is no larger than a small power of the product of the *distinct* primes dividing the product ABC.

Consider the cubic curve $\mathcal{E}_{a,b,c} : y^2 = x(x - a)(x + b)$, where $a + b = c$ in distinct integers. With that condition on a, b and c we have a 'Frey curve' $\mathcal{E}_{a,b,c}$, an elliptic curve with discriminant essentially abc. In 1985 Frey had remarked that, for $uvw \neq 0$ and $p \geq 5$, if $2 \big| u$ and $v \equiv 1 \bmod 4$ then the curve $\mathcal{E}_{u^p,v^p,w^p}$ is semistable and its supposed existence seemed likely to contradict the Modularity Conjecture of Taniyama–Shimura for elliptic curves over the rationals $\mathbb{Q}$. In the language of the seventies, $\mathcal{E}_{u^p,v^p,w^p}$ could apparently not be a Weil curve. A suggestion of Serre, his ε–Conjecture, was proved by Ribet in 1986, entailing that indeed the truth of the Modularity Conjecture, and then just for semistable elliptic curves, implies Fermat's Last Theorem. At the time, though, it was believed that the Modularity Conjecture was inaccessible; that its proof was at least a generation away.

Now. It was therefore an enormous surprise and excitement when, at Cambridge University in 1993, Andrew Wiles, a British mathematician by then working at Princeton, announced he had proved Fermat's Last Theorem by establishing the Modularity Conjecture for semistable elliptic curves over $\mathbb{Q}$. There followed a year or so of alarums in which a subtle gap in the argument had to be filled. In 1995 a paper of Wiles, augmented by a further joint note with Richard Taylor, finally proved Fermat's allegation.

Fittingly, Fermat's Last Theorem was proved as a corollary of far more fundamental results.

The proof of Fermat's Last Theorem *is* important. A reasonable comparison is to suggest that it's as important to mathematics as the landing on the moon was to science and technology. The proof is as dramatic as the landing, and as exciting to the onlookers. Of itself, knowing that Fermat's claim is true barely advances mathematics, but then the actual taking of people to the moon did not hugely add to our scientific knowledge. The moon landing was the corollary, as it were, to a long and steady scientific and technological advance, punctuated by occasional dramatic breakthroughs. The landing was not itself such a breakthrough. In that spirit, Fermat's Last Theorem is a culmination of some 350 years, well certainly 250 years, of mathematical advance. However, Wiles' work does constitute a dramatic advance, one of those special watersheds. The great advance lies in his showing that, indeed, the Modularity Conjecture of Taniyama–Shimura–Weil is true, at any rate for semistable elliptic curves. This confirms that the experimental and contextual evidence had not led mathematics astray. If the "Holy Grail" of Fermat's Last Theorem was needed to motivate that advance, well that's fine. There will have been worse reasons for advancing mathematics.

The future. So, what remains? At much the time of Wiles' announcement, Darmon and Granville had proved that Faltings' Theorem implies that the equation $x^r+y^s = z^t$ has at most finitely many solutions in relatively prime integers x, y and z; this provided that $1/r+1/s+1/t < 1$. The case where the sum of the reciprocals of the exponents is 1 includes Fermat's Last Theorem with exponents 3, and 4 — the latter via the case $(2, 4, 4)$. When the sum is greater than 1, Beukers has shown there are infinitely many solutions parametrised by finitely many sets of polynomials in several variables. There are ten known solutions in the interesting case, starting with $3^2 - 2^3 = 1^7$, say, and with largest solution $43^8 + 96\,222^3 = 30\,042\,907^2$. In all ten solutions at least one of the exponents is 2. So now we may have the *Generalised Fermat Conjecture* that the Darmon–Granville equation has no solutions with all exponents larger than 2. One should not dare suggest that the ten known solutions *are* all the primitive solutions. Yet it remains intriguing that these solutions do not contradict the GFC.

The worthwhile question for mathematics however is the ABC-conjecture. There is growing indication that it implies just those facts one would conjecture anyhow on more reliable grounds. Moreover, here we can prove an analogue in function fields. Though such arguments are not transferable to the arithmetic case, they have proved most reliable in suggesting what *is* the truth in that case.

References. For the legends see [A1]; the more recent [A2] also does not involve any actual mathematics. Kummer's work is introduced and detailed in [B] at advanced

undergraduate level, whilst [C] inter alia gives near complete references to work on the FLT up to the 1970's. Finally, [D] provides an accessible introduction to Wiles' proof 'in an amusing and intriguing collection of tidbits, anecdotes, footnotes, exercises, references, illustrations, and more'. The collection [E] is at workshop level, with extensive details and explanation of the proof and the mathematics underlying it. The proof itself appears in the pair of papers [F].

[A1] Eric Temple Bell, *The Last Theorem*, Mathematical Association of America, Washington, 1990.

[A2] Simon Singh, *Fermat's Enigma : The Quest to Solve the World's Greatest Mathematical Problem*, Walker & Co, 1997

[B] Harold M Edwards, *Fermat's Last Theorem — A genetic introduction to algebraic number theory*, Springer–Verlag, 1977

[C] Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer–Verlag, 1979

[D] Alf van der Poorten, *Notes on Fermat's Last Theorem*, Wiley–Interscience 1996

[E] Gary Cornell, Joseph H. Silverman and Glenn Stevens eds., 'Modular Forms and Fermat's Last Theorem', Springer–Verlag, 1997.

[F] Andrew Wiles, 'Modular elliptic curves and Fermat's Last Theorem' *Ann. Math.* (ser. 2) **141** (3), 443–551 ;

Richard Taylor and Andrew Wiles, 'Ring-theoretic properties of certain Hecke algebras' *ibid.*, 553–572.

A J van der Poorten, Sydney, 1998