Notes on Fermat's Last Theorem

LECTURE I

The story of "Fermat's Last Theorem"
has been told so often it hardly bears retelling.
H. M. Edwards

Dramatis Personæ:

Euclid of Alexandria	~ −300
Diophantus of Alexandria	~ 250
Pierre de Fermat	1601–1665
Leonhard Euler	1707–1783
Joseph Louis Lagrange	1736–1813
Sophie Germain	1776–1831
Carl Friedrich Gauss	1777–1855
Augustin Louis Cauchy	1789–1857
Gabriel Lamé	1795–1870
Peter Gustav Lejeune Dirichlet	1805–1859
Joseph Liouville	1809–1882
Ernst Eduard Kummer	1810–1893
Harry Schultz Vandiver	1882–1973
Gerhard Frey	
Kenneth A. Ribet	
Andrew J. Wiles	

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

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

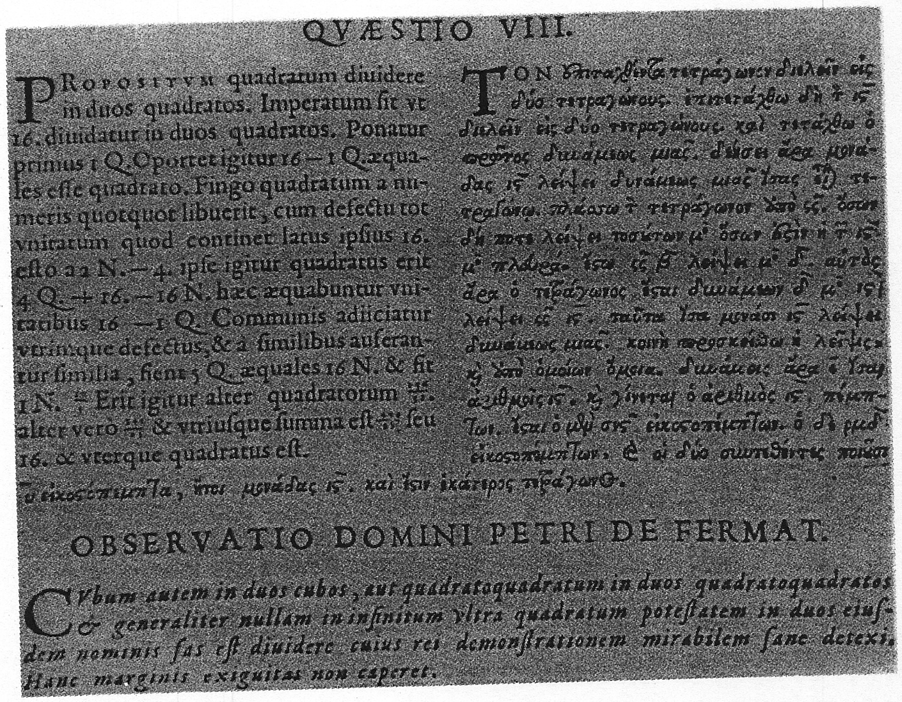
if n is an integer greater than 2. For n equals 2 there are many solutions:

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

the Pythagorean triples. In the margin of his copy of the *Arithmetica* of Diophantus the French jurist Fermat wrote *circa* 1637 that for greater n no such triples can be found; he added that he had a marvelous proof for this, which however the margin was too small to contain:

> *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.*

Every other result which Fermat had announced in like manner had long ago been dealt with; only this one, the *last*, remained.



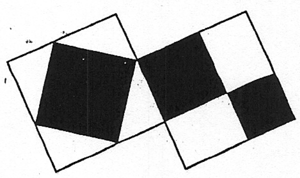
QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. 16/5. Erit igitur alter quadratorum 256/25. alter verò 144/25 & vtriusque summa est 400/25 seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Problem 8 in Book II of Claude Bachet's translation of Diophantus asks for a rule for writing a square as the sum of two squares. The resulting equation $z^2 = y^2 + x^2$ is that of the Theorem of Pythagoras, which says that in every right-angled triangle the square on the hypotenuse is the sum of the squares on the other two sides. The logo of Macquarie University's ceNTRe for Number Theory Research



provides a graphical proof; we see that Pythagoras's Theorem has only the depth of the familiar quadratic identity $(x+y)^2 = x^2 + 2xy + y^2$.

It is a little more difficult to find all solutions in integers, but not much more. If $x^2 + y^2 = z^2$, we can suppose that x, y, and z pairwise have no common factor, for such a factor would be common to all three quantities and can be factored out, leaving an equation of the original shape. Thus at least two of x, y and z must be odd. But the square of an odd number, so of the shape $(2m+1)^2 = 4m^2 + 4m + 1$, leaves a remainder of 1 on division by 4 (and on division by 8), while the square of an even number, so of the shape $(2m)^2 = 4m^2$, leaves a remainder of 0 on division by 4. It follows that z must be odd and that one of x and y, say $x = 2x'$, must be even. Then we obtain

$$4x'^2 = z^2 - y^2 = (z+y)(z-y) \quad \text{so} \quad x'^2 = \tfrac{1}{2}(z+y)\tfrac{1}{2}(z-y).$$

But if the product of two numbers that have no factor in common is a square, then each of the two numbers is a square.

This is clear on splitting the two numbers into their prime factors and checking the contribution of each distinct prime. To apply the principle we need only note that both $\frac{1}{2}(z+y)$ and $\frac{1}{2}(z-y)$ are integers, because both z and y are odd; and that they have no common factor. The latter is evident, because if d were a common factor, then d is a factor both of their sum z, and their difference y. Yet we began by determining that y and z are *relatively prime* — that they have no common factor. So both $\frac{1}{2}(z+y)$ and $\frac{1}{2}(z-y)$ are squares, say

$$\tfrac{1}{2}(z+y) = u^2 \quad \text{and} \quad \tfrac{1}{2}(z-y) = v^2.$$

Thus $x'^2 = u^2v^2$. Summarizing, we have

$$x = 2uv, \quad y = u^2 - v^2, \quad \text{and} \quad z = u^2 + v^2.$$

We obtain all Pythagorean triples without common factor by choosing integers u and v without common factor and of different *parity* — that is, one odd and the other even, and with u greater than v.

Of course, it is easy to verify that indeed

$$(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2.$$

Fermat did show that the equation

$$x^4 + y^4 = z^4$$

has no solution in positive integers. In fact, he shows a little more, that already

$$x^4 + y^4 = w^2$$

has no solution in positive integers. As above, we may suppose that x is even, and y and w are odd. Then by the preceding argument, it follows that there are integers a and b so that

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad \text{and} \quad w = a^2 + b^2.$$

From the expression for y^2 it follows that a is odd and b is even, and from that for x^2 we may deduce that there are integers c and d so that

$$a = c^2 \quad \text{and} \quad b = 2d^2 .$$

Hence

$$y^2 = c^4 - 4d^4 .$$

Again applying the results from the case $n = 2$ we see that there are integers e and f so that

$$y = e^2 - f^2 , \quad d^2 = ef \quad \text{and} \quad c^2 = e^2 + f^2 .$$

Clearly, e and f must be relatively prime, so there are integers u and v such that

$$e = u^2 , \quad f = v^2 , \quad \text{and} \quad u^4 + v^4 = c^2 .$$

But now Fermat makes a truly marvelous observation. He notes that c is less than w. So what this argument shows is that given a solution (x, y, w) there is a *smaller* solution (u, v, c) ! That is, eventually, absurd. By the *method of infinite descent*, here introduced, it follows that there is no solution in positive integers to $x^4 + y^4 = w^2$, and *a fortiori* — all the more so, none for $x^4 + y^4 = z^4$.

It was many years later, in 1753, that Euler dealt with the case $n = 3$. There was an alleged error in the argument, later dealt with 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.

On 1 March, 1847, Lamé informed the Parisian *Académie des Sciences* that he had settled the general case. Lamé attributed the basic idea of his proof to Liouville. The idea consisted of working with numbers of the shape

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1} ,$$

where $a_0, a_1, \ldots, a_{n-1}$ are integers and ζ is a complex number with the property that $\zeta^n = 1$, but $\zeta \neq 1$. Here Lamé assumed n to be an odd prime number. It had been known for some time that this assumption does not, of course, impose any restriction in the proof of Fermat's Last Theorem.

With the aid of these numbers, $x^n + y^n$ may be split into n factors:

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y)$$

and Fermat's equation then assumes the shape

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y) = z^n .$$

To this Lamé applies a generalization of the principle already described in the case $n = 2$, whereby if a product of numbers without common factor is an nth power, then each is an nth power. Lamé assumes that this principle holds for the *cyclotomic* integers he has just introduced and proceeds with an argument showing necessarily one of x or y to be zero.

After Lamé, Liouville addressed the meeting. He pointed out that the idea of using complex numbers was nothing new; one could already meet such numbers in the work of Euler, Lagrange, Gauss, and Jacobi. Moreover, it seemed to him, said Liouville, that Lamé implicitly assumed that unique factorization into primes also held for cyclotomic integers.

A second difficulty is numbers that divide 1, or *units* as we now call them. There is a problem, in that, for example, $-4 \times -9 = 36$, with 36 a square and -4 and -9 relatively prime, while neither is a square. In the cyclotomic case one can see readily that there are many more units than just ± 1. For example, $\zeta + \zeta^{n-1}$ is a unit whenever $n > 1$ is odd. Properties of divisibility by $\zeta + \zeta^{n-1}$ play an important role in Lamé's argument. But $\zeta + \zeta^{n-1}$ divides 1, and therefore every number.

N'y a-t-il pas là une lacune à remplir?
J. Liouville

Some of this material has been liberally borrowed from the introduction to the thesis of Hendrik Lenstra, Jr., 'Euclidean number fields', *Math. Intelligencer* 2 (1980), pp. 6–15, 73–77, 99–103; that work is Copyright © 1980 Springer-Verlag New York, Inc. and is partly reprinted here with permission. The rest comes from things I just knew and from notes of mine of some 17 years ago which were probably much aided by thoughts learned from W. J. LeVeque, *Topics in Number Theory*, (Reading, Mass.: Addison-Wesley 1961), Vol 2.

Notes and Remarks

I.1 The style I have adopted here is to *announce* all sorts of things. Some announcements are just definitions, others are facts whose explanations we are not yet in a position to comprehend. Many of my claims are indeed obvious after one has thought just a little while. Mostly, these accessible claims are signalled by such phrases as "we see that", "it is now obvious that", "clearly", and the like. Throughout, the exercises for the reader are to supply the extra remark needed to make my claims totally obvious, or to explain why my hints really make my claim immediate. But just in case there is not enough to do, let me add a few remarks.

I.2 In that notorious margin, Fermat writes that 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 that he has a marvelous proof for this. But the margin is too narrow to contain it.

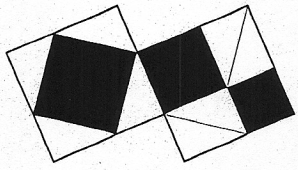
His failure to provide a proof is not significant. Most of what we know of Fermat's work derives from the challenges he puts to his correspondents; by and large we can reconstruct the arguments from detailed hints. The Last Theorem, however, does not remain the subject of such challenges

and it seems plain* that Fermat quickly realizes that he has an argument at most in the case $n = 4$, and perhaps $n = 3$.

I.3 The appearance in 1621 of the translation into Latin of the then extant books of Diophantus signals the beginning of modern number theory. We owe the infamous Last Theorem to Fermat's son Samuel, who in 1670 reprinted his father's copy of Bachet's Diophantus, together with the marginal notes.

I.4 The Macquarie University Number Theory Reports explain on their inside cover that

> The logo for ceNTRe depicts an elegant proof of the theorem of Pythagoras, which states that the area of the square drawn on the hypotenuse of a right angled triangle is equal to the sum of the areas of the squares drawn on the other sides. This result was known to the ancient Babylonians who used it to construct accurate right angles. In the logo, reproduced below with two additional construction lines, the two larger squares each contain four identical right angled triangles, and have sides of the same length, namely the sum of the lengths of the two shorter sides of the right angled triangles. Thus the remaining area in the two squares are equal. In the left hand square, this area is the area of the square drawn on the hypotenuse of the right angled triangle. In the right hand square it is the sum of the areas of the squares drawn on the other two sides.



> The sides of the three solid squares in the logo are in the ratio 3:4:5, corresponding to the well known right angled triangle. It also corresponds to the simplest non-trivial solution in integers of the equation $X^2 + Y^2 = Z^2$. Integer solutions of equations such as these play an important role in modern number theory.

*Weil, in his *Number Theory: An approach through history. From Hammurapi to Legendre*, (Basel, Switzerland: Birkhäuser 1984), remarks at p104 that "for a brief moment he [Fermat] must have deluded himself into thinking that he had the principle of a general proof; what he had in mind on that day can never be known."