
Timothy O'Neil

Catalan's Equation

During the Summer of 1993, a great deal of attention was paid by the media to some marvelous results from Professor Andrew Wiles, which led to a proof of Fermat's Last Theorem. Suddenly, many people who would never admit to any mathematical ability were paying homage to Fermat and his result. Unfortunately, gaps soon appeared in Wiles' work which took a few months to fill. Finally, as shown in [1] and [2], we are able to eliminate Fermat's Last Theorem as the most famous unsolved problem in mathematics.

Running well behind Fermat's Last Theorem is Catalan's Conjecture. Both give rise to Diophantine Equations (that is, exponential-polynomial equations with solutions over the integers); both have seen considerable time and effort expended on them in the name of discovering the secrets they hide; and both have jealously concealed their secrets from prying eyes for centuries. Their difference comes in their solutions. Fermat's Last Theorem is now completely solved, while the answer to Catalan's question is solved only in principle.

Our purpose in this note is to discuss the history of Eugene Catalan and his problem; to examine the similar paths that research on the two problems has taken; and finally, to see where the paths diverge so that we may understand why Catalan's Problem is still not completely solved while Fermat's Last Theorem is.

The Two Problems Stated

As we have observed above, both problems can be described by equations to be solved over the integers. Fermat's Last Theorem is that there are no solutions to

$$d^n + b^n = c^n \tag{1}$$

Timothy O'Neil will resume his doctoral work in Computer Science at the University of Notre Dame this fall. From 1996 to 1998, he taught computer science and mathematics courses at Manchester College in Indiana. Prior to that, he studied number theory with Andrew Glass at Bowling Green State University (Ohio). He is deeply indebted to Barbara Moses of BGSU for her assistance in completing this article.

in the set of positive integers when n is an integer greater than 2. On the other hand, Catalan's Conjecture is that there are no solutions to

$$a^p - b^q = 1 \quad (2)$$

in the set of positive integers when p and q exceed 1 except for the case where $a = q = 3$ and $b = p = 2$.

Catalan and His Problem

The origins of what we now know as Catalan's Equation go back to the 14th Century, when Lewi ben Gerson (writing in Latin under the pseudonym Leo Hebreus) proved that $3^m \pm 1$ has an odd factor when $m > 2$. This implies that (2) has no solution when $a = 2$ and $b = 3$ except for the one we've noted.

About five hundred years later, in 1814, Eugene Charles Catalan was born in Brugge (Bruges), Belgium. He received his degree in 1841 from l'Ecole Polytechnique, the prestigious Parisian university, and stayed in France to teach for many years at Charlemagne College (participating in the Revolution of 1848 in his spare time) before returning home to a professorship at Liege. Over the course of his career, Catalan did work in analysis (studying differential equations and power series), differential geometry (in 1843 he published his research on the surface that today bears his name) and number theory. So noted was he for his work in number theory that he served the Belgian Academy of Science in 1883 as one of three referees in charge of administering a prize for a proof to Fermat's Last Theorem. Catalan died in 1894.

Equation (2) came to bear Catalan's name as a result of his letter to the editor of Crelle's Journal, wherein he wrote (translated here from the French):

I beg you, sir, to please announce in your journal the following theorem that I believe true although I have not yet succeeded in completely proving it; perhaps others will be more successful. Two consecutive whole numbers, other than 8 and 9, cannot be consecutive powers; otherwise said, the equation $x^m - y^n = 1$ in which the unknowns are positive integers only admits a single solution.

This letter appeared on the front page of Crelle's Journal in 1844. The legend was born.

Solutions for Individual Exponents

We will start from the beginning in comparing the similar paths research on the two problems has taken. Fermat left the statement of his "Last Theorem" in notes found posthumously in 1665. Among these was Fermat's only proof on the subject: that (1) has no solution in the set of positive integers when $n = 4$. This was the early pattern—to try to eliminate individual exponents n , hoping to develop some insight which would lead to a general solution.

Now it is clear that, for both (1) and (2), we need only concern ourselves with prime exponents. For example, if (1) had an integral solution for $n = pq$, where p is prime, then it has one for this prime exponent p , since then

$$(a^q)^p + (b^q)^p = (c^q)^p$$

With this in mind, Euler eliminated $n = 3$ in 1770, Dirichlet and Legendre removed $n = 5$ in 1825 and Lamé got rid of $n = 7$ in 1839 [2].

The early research on Catalan's problem followed a similar pattern, but with more limited success. After all, it is harder to examine individual exponents in (2). Also, by the time Catalan's Conjecture was being explored, it was known that this "generalization" approach had not worked for Fermat's Equation, and so didn't look promising for solving Catalan's. Nonetheless, the obvious question was considered; since (2) has a solution when both $p = 2$ and $q = 3$, is there a solution when just one of these is true? The answer is no. In 1850, Lebesgue showed that when $q = 2$ and $p \neq 3$ in (2), there is no solution. Further, Nagel showed in 1921 that when either p or q is 3 in (2), the other exponent must be 2 for a solution to exist. However, it took until 1964 to finish this line of questioning, when Chao Ko demonstrated that there is no solution to (2) when $p = 2$ and $q \neq 3$ [4].

The Two Cases of Fermat

In 1827, Legendre [3] published a result by Sophie Germain which contributed the next significant advance in the quest for a solution to (1). What Germain did was divide Fermat's Last Theorem into two cases: Case I, in which the exponent n divides none of a , b or c ; and Case II, in which n does divide one of these quantities. Between them, Germain and Legendre demonstrated that (1) has no solution for prime exponent n less than 197 when Case I is assumed. This result preceded Lamé's for $n = 7$ by eleven years. It was apparent that the focus of future research on the problem should shift from examining individual exponents to trying to completely crack Cases I and II separately.

This approach was applied by Cassels in 1960 to Catalan's equation and resulted in a significant discovery: there is no Case I for Catalan. That is, Cassels demonstrated that, if (2) has a solution, then p divides b and q divides a .

The Wieferich Condition

By the turn of the century, research into Fermat's Last Theorem came to a temporary halt. Kummer's work in the 1850s, while very significant in its own right, had failed to completely solve the problem. Additionally, the proliferation of cash prizes offered for a complete solution was about to lead only to a golden age of bogus proofs.

The German Wieferich stepped into this fray in 1909. Assuming Case I of Fermat, Wieferich [5] showed that, if n is prime and

$$2^{n-1} \equiv 1 \pmod{n^2}$$

then (1) does not have a solution in integers. By itself, this result eliminated all possible exponents $n < 6 \times 10^9$ except for $n = 1093$ and 3511 . These fell the next year, when Mirimanoff [5] showed Wieferich's result with the "2" replaced by a "3". Over the years, researchers have shown that this "2" can be replaced by any prime smaller than 104, eliminating Case I for all exponents $n < 2.3 \times 10^{19}$.

A corresponding result for the Catalan equation was discovered by Inkeri [6]. In several papers published in the years 1964 to 1991, he showed that, if either

$$p^{q-1} \equiv 1 \pmod{q^2} \text{ or } q^{p-1} \equiv 1 \pmod{p^2}$$

then (2) has no integral solution for exponents p and q . The reader should note that this is a simplification of Inkeri's results. While true most of the time, there are a few exceptional cases which cannot be eliminated using this theorem; as reported in [7] and [8], they involve divisibility by q of the class number of the maximal subfield of the cyclotomic field of $(x^p - 1)/(x - 1)$ which has dimension a power of 2 (and with p and q interchanged).

Fermat's Last Theorem Proved

The work of Wiles in fact began about thirty years ago, when Taniyama and Shimura [9] conjectured that all elliptic curves are modular. The importance of this became clear when Kenneth Ribet [9] showed that, if there is an ordered triple (a, b, c) which satisfies (1) then the elliptic curve

$$y^2 = x(x - a^n)(x + b^n) \tag{3}$$

is not modular. So if Taniyama and Shimura are right, Fermat's Last Theorem is an easy corollary. What Wiles proved is that all semi-stable elliptic curves are modular. Thankfully (3) or an isomorphic copy of (3) is semi-stable, so this is enough. On the other hand, (2) yields the semi-stable elliptic curve

$$y^2 = x(x - a^p)(x - b^q)$$

where the ordered quadruple (a, b, p, q) satisfies (2). However, in contrast with (3), there is no reason for it to be non-modular, so no obvious contradiction arises.

Tijdeman's Result

Another significant difference between the theorems of Fermat and Catalan came as a result of Tijdeman's work in 1976. It had been known since 1929 that (2) only has a finite number of solutions over the integers, a discovery due to Siegel [10]. What Tijdeman did was apply Baker's ground-breaking work of the mid-1960s to Catalan's Equation to show that there is some computable number C so that, if x , y , p and q satisfy (2), then all of these quantities are smaller than C .

The importance of this result cannot be understated, since it greatly limits our universe. Unlike solutions to Fermat, which can potentially occur anywhere, solutions to Catalan occur only within a limited interval. In principle, all that is now necessary is a vast computer search. If we can make this interval small enough (by making our constant C sufficiently small), we can perform a search via computer, developing a small list of possible exponents for (2) which meet both Inkeri's criteria and fall within the required bounds. The bad news is that C needs a lot of work. The original calculation, due to Langevin [10], sets C equal to $\exp(\exp(\exp(\exp(730))))$.

Conclusion

The current best bounds for (2), reported in [11], require that $\max\{p,q\} < 4.13 \times 10^{17}$ and $\min\{p,q\} < 3.31 \times 10^{12}$. (They arise from improvements in the constants for linear forms in 2 and 3 logarithms of algebraic numbers due to Baker, Laurent, Mignotte, Nesterenko, Waldschmidt, Wustholz, and a team at Bowling Green State University in Ohio.) As time progresses, eventually these bounds will be small enough and computer technology fast enough that a systematic search can be performed, identifying those pairs of prime exponents for (2) which pass Inkeri's test. Once all such pairs are identified, other ideas will be needed in order to either eliminate all exceptions or discover an additional solution to (2).

So don't be surprised if you also hear about a solution to Catalan's problem within the next few years. The complete answer may be just around the corner.

References

1. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics, **141** (1995), 553--572.
2. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics, **142** (1995), 443-551.
3. H. Edwards, *Fermat's Last Theorem: A genetic introduction to algebraic number theory*. Springer-Verlag, New York, 1977.
4. P. Ribenboim, *Catalan's conjecture: Are 8 and 9 the only consecutive powers?*, Academic Press, New York, 1994.
5. P. Ribenboim, *The little book of big primes*, Springer-Verlag, New York, 1991.
6. K. Inkeri, *On Catalan's problem*, Acta Arithmetica, **9** (1964), 285-

290.

7. M. Mignotte, *A criterion on Catalan's Equation*, Journal of Number Theory, **52** (1995), 280-284.

8. W. Schwarz, *A note on Catalan's Equation*, Acta Arithmetica, **72** (1995), 277-281.

9. A.M.W. Glass, *Constants for linear forms in three and four logarithms*, Ulam Quarterly, to appear.

10. M. Waldschmidt and J. Velu, *Les victoires de la transcendance*, La Recherche, **8** (1977), 1059-1065.

11. T. O'Neil, "Improved Upper Bounds on the Exponents in Catalan's Equation", submitted.

Additional Sources

L.E. Dickson, *History of the theory of numbers*, Volume II, G.E. Stechert and Company, New York, 1934.

Encyclopedia of Mathematics, Volume 2, Kluwer Academic Press, Dordrecht, The Netherlands, 1988.

J. Fang, *Mathematics from antiquity to today*, Volume 1, Paideia Press, Hauppauge, NY, 1972.