THE LATEST ON CATALAN'S CONJECTURE

Andrew Granville

If one writes the sequence of squares, cubes and higher powers of integers in increasing order:

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, \ldots$$

one notices that they become increasingly sparse. As far as out as one could conceivably compute one finds that the smallest gaps between consecutive powers become larger and larger, and indeed 8 and 9 seem to be the only consecutive integers in this sequence. In a letter to Crelle's journal in 1844, Catalan noticed this and wrote "I believe that this is true, though I have not yet given a complete proof; others perhaps will be more lucky". A precise statement of what is now known as **Catalan's conjecture** goes as follows: *The only solution to*

$$X^m - Y^n = 1 \tag{1}$$

in integers $X, Y, m, n \geq 2$ *is* $3^2 - 2^3 = 1$. To this day Catalan's conjecture remains unanswered though, as I shall report in this article, researchers are coming tanatalizingly close to showing that Catalan was indeed correct.

To begin with note that if there is a solution to the above equation where prime p divides m and prime q divides n then

$$x^p - y^q = 1 \tag{1'}$$

with $x = X^{m/p}$ and $y = Y^{n/q}$. Thus Catalan's conjecture can be re-phrased as stating that there are no solutions to (1') in integers $x, y > 1$ and primes p and q. With this observation in hand let us begin by surveying the key results known before the most recent attacks on this famous problem:

The first recorded result on Catalan's conjecture came over five hundred years before Catalan's letter: Levi ben Gerson (1288–1344) showed that the only powers of 2 and 3 that differ by 1 are indeed $3^2 - 2^3 = 1$ (note that we don't mention any of the solutions $2^2 - 3^1 = 3^1 - 2^1 = 2^1 - 3^0 = 1$ since in each case at least one of the exponents is less than 2). Roughly a hundred years before Catalan's letter, Euler in 1738 showed that the only square and cube (of rational numbers) that differ by 1 are $3^2 - 2^3 = 1$.

In 1850 Lebesgue showed that there are no solutions when $q = 2$ in (1'), and in 1964 Chao Ko showed that there are no solutions when $p = 2$ in (1'), except of course $3^2 - 2^3 = 1$. In 1921, Nagell showed that there are no solutions in (1') when $p = 3$ or $q = 3$ (except the ubiquitous $3^2 - 2^3 = 1$).

Typeset by $\mathcal{AMS}$-TEX

Therefore we can now assume that $p, q \geq 5$. By 1961 Cassels had shown that for any solution in (1') we have that p divides y, and q divides x, which gives us that we can write

$$\begin{aligned} x-1 = p^{q-1}a^q \quad &\text{and} \quad \frac{x^p-1}{x-1} = pu^q \\ y+1 = q^{p-1}b^p \quad &\text{and} \quad \frac{y^q+1}{y+1} = qv^p \end{aligned}$$

where a, b, u and v are integers for which $(pa, u) = (qb, v) = 1$, with $x = qbv$ and $y = pau$.

In 1929 Siegel showed that any curve of genus > 0 has only finitely many integer points: In our example this means that if we fix primes $p, q \geq 2$ then there are only finitely many integers x and y satisfying (1'). Unfortunately Siegel's proof does not give us any hint how to restrict the possible values of x and y in such a way that we can mount a search and find all solutions. It was not until Baker's Fields' medal winning work, in the sixties, on linear forms in logarithms that it was possible to bound the sizes of x and y, in terms of p and q, though the bounds that come directly out of his technique were so large as to be uncomputable in practice. Nonetheless it was Baker's work that heralded the more recent assaults on Catalan's conjecture, and indeed in 1976 Tijdeman, using Baker's Theorem, showed that x^p (and so y^q) are bounded by some computable absolute constant in any solution of (1'). A succession of authors computed such a constant, trying to make it so small that all examples in (1') might then be found by a practical computer search.

The latest upper bounds are (according to Mignotte) $\min\{p, q\} < 7.15 \times 10^{11}$ and $\max\{p, q\} \leq \max\{m, n\} < 7.78 \times 10^{16}$ — as we shall see later, upper bounds on x and y are unlikely to be important in the eventual resolution of Catalan's conjecture so we will not write them out, though in principle they could be written out.

Fermat's Last Theorem and Catalan's equation

Wiles, of course, recently proved Fermat's Last Theorem, that there are no positive integers x, y, z and prime $p > 2$ for which

$$x^p + y^p = z^p. \tag{2}$$

There is much in common between these two famous problems, and indeed several of the techniques used on Fermat's Last Theorem, over the three and a half centuries in which it was an unsolved problem, can be adapted to Catalan's Conjecture. Most important pre-Wiles results on Fermat's Last Theorem involved an in-depth understanding of the arithmetic of the pth cyclotomic field, that is the field generated by the rational numbers and the pth roots of unity (this is because $x^p + y^p$ factors into linear factors in this field). One famous such result on (2), by Kummer in the middle of the nineteenth century, is that if p does not divide the class number of the pth cyclotomic field then there are no solutions to (2). Another, by Wieferich in 1910, that unless $2^{p-1} \equiv 1 \pmod{p^2}$, then p divides xyz in any solution to (2). Note that although $2^{p-1} \equiv 1 \pmod{p}$ for every odd prime

p, it is very rare that this congruence holds $\pmod{p^2}$ (indeed only for $p = 1093$ and $p = 3511$ of the primes $p < 2^{32}$). Subsequent authors showed that the '2' in $2^{p-1} \equiv 1 \pmod{p^2}$ can be replaced by '3', '5' or any odd prime up to '109' (and feasibly beyond, though to prove such a result for $q^{p-1} \equiv 1 \pmod{p^2}$ for any given prime q seems to require a prohibitively lengthy computation when q is large).

Since $x^p - 1$ also factors in the pth cyclotomic field, and $y^q + 1$ factors in the qth cyclotomic field one might guess that analogous results could be proven for (1'). In 1964 Inkeri figured out how to do this obtaining criteria involving class numbers *and* "Wieferich-type congruences". In the last decade there have been several papers trying to simplify Inkeri's results (and approach). Ultimately, though, it was an amateur mathematician, Preda Mihăilescu, who works for a fingerprinting company in Switzerland, who put Inkeri's idea into perhaps its ultimate form. In a paper just accepted by the *Journal of Number Theory*, he shows that if there is a solution to (1') then

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

Grantham and Wheeler have computed the only such "Wieferich pairs" with $3 < p, q < 3 \times 10^8$: there are a few (such as $(5, 1645333507)$, $(83, 4871)$, $(2903, 18787)$ and $(911, 318917)$), though we expect very few overall. (Mihailescu also showed that q^2 divides x and p^2 divides y, improving on Cassels). By rather different considerations, Bugeaud and Hanrot (adapting ideas of Bilu and Hanrot) show that if there is a solution to (1') and $q > \frac{p}{2} \cdot \left(1 + \frac{1}{\log q}\right)$ then q divides $h^-(p)$, the "relative class number" of the pth cyclotomic field: This is easier to compute then the actual class number, and none of the Wieferich pairs listed above satisfy this criteria. Thus we know that in any unknown solution to (1'), p and q are both greater than three hundred million.

Therefore we now know that $p, q > 3 \times 10^8$ and $m, n < 7.78 \times 10^{16}$, so that $m < p^2$ and $n < q^2$. That means that $m = p$ and $n = q$; that is, in any solution to (1), m and n must both be prime! In any unknown solution to (1') we now have $3 \times 10^8 < \min\{p, q\} < 7.15 \times 10^{11}$ and $\min\{p, q\} < \max\{p, q\} < 7.78 \times 10^{16}$. This range seems to be close to what might be feasible computationally: A fairly straightforward algorithm could check all the remaining pairs in something like 10^{30} steps, not too far beyond what is practical, but far enough that one expects additional ideas will be needed before a final computer onslaught will be successful.

The Fermat-Catalan equation

With the solution of Fermat's Last Theorem, and perhaps of Catalan's Conjecture in the very near future, we might ask what is the next big question of this flavor. My own personal favorite is

The Fermat-Catalan Conjecture. *There are only finitely many triples of co-prime integer powers x^p, y^q, z^r, for which*

$$x^p + y^q = z^r \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1. \tag{3}$$

This generalizes both (1') and (2). From "classical" results we know that the only solution when $1/p + 1/q + 1/r = 1$ is $1^6 + 2^3 = 3^2$. There are ten solutions

(x, y, z) known to the above equation:

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,$$

$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$

$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

Perhaps these are all. Noting that all of these solutions involve an exponent '2', might lead one to conjecture that there are no solutions to $x^p + y^q = z^r$ in coprime integers x, y, z when p, q, r are all > 2. This conjecture was made by Dallas banker Andrew Beal who subsequently offered a substantial cash reward ($ 50,000) for its resolution!

Darmon and I showed that for any fixed such p, q, r there are only finitely many such solutions to (3), as a consequence of a deep theorem of Faltings. Important cases for which the conjecture is known to be true are: $p = q = r$ (Wiles), $p = q$ and $r = 2$ or 3, as well as $p = r = 4$ (Darmon and Merel), $p = q = 3$ (Kraus), $\{p, q, r\} = \{2, 4, 5\}, \{2, 4, 6\}$ and $\{2, 3, 8\}$ (Bruin), all using interesting, deep ideas. Darmon has outlined a program to modify Wiles' approach to Fermat's Last Theorem, to prove the Fermat-Catalan Conjecture. His ambitious ideas, though impractical at the moment, boldly set a direction for future attacks on such problems.

References

[1] Yann Bugeaud and Guillaume Hanrot, *Un nouveau critère pour l'équation de Catalan* (to appear).

[2] J.W.S. Cassels, *On the equation $a^x - b^y = 1$, II*, Proc. Camb. Phil. Soc. **56** (1960), 97-103.

[3] Kustaa Inkeri, *On Catalan's problem*, Acta Arith **9** (1964), 285-290.

[4] Alain Kraus, *On the equation $x^p + y^q = z^r$*, Ramanujan J **3** (1999), 315-333.

[5] Michel Laurent, Maurice Mignotte and Yuri Nesterenko,, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. of Number Theory **55** (1995), 285-321.

[6] Maurice Mignotte, *Catalan's equation just before 2000* (to appear).

[7] Preda Mihăilescu, *A Class Number Free Criterion for Catalan's Conjecture*, J. of Number Theory (to appear).

[8] Paulo Ribenboim, *Catalan's conjecture*, Academic Press, 1994.

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu