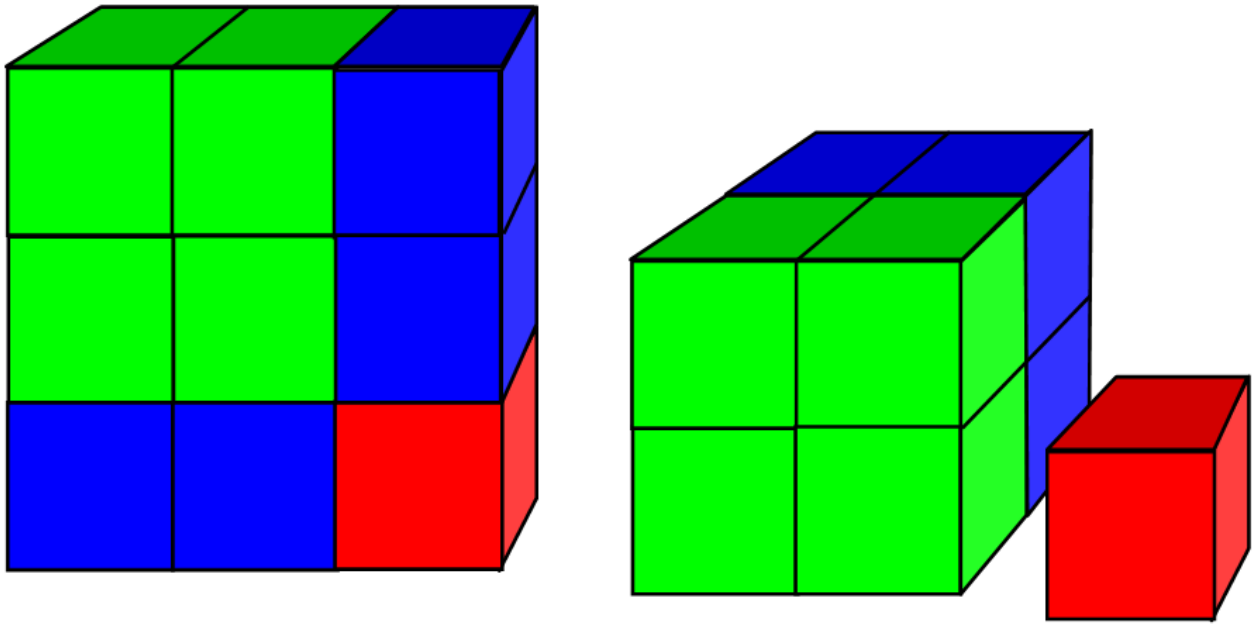
THEOREM OF THE DAY

Catalan's Conjecture (Mihăilescu's Theorem) *Let x, y, p, q be positive integers satisfying $x^p - y^q = 1$. Then $x = q = 3$ and $y = p = 2$.*



Catalan 'near misses'

$x^p - y^q \leq 10$, $2 \leq x, y, p, q \leq 100$, p, q, prime

$3^3 - 5^2 = 2$

$2^7 - 5^3 = 3$

$2^3 - 2^2 = 6^2 - 2^5 = 5^3 - 11^2 = 4$

$2^5 - 3^3 = 5$

$2^5 - 5^2 = 4^2 - 3^2 = 2^7 - 11^2 = 7$

$4^2 - 2^3 = 8$

$5^2 - 4^2 = 6^2 - 3^3 = 15^2 - 6^3 = 9$

$13^3 - 3^7 = 10$

In other words, 8 and 9 are the only nontrivial instance of consecutive perfect powers. We may restrict attention to prime powers since a solution to, say, $x^4 = y^{15} + 1$, would give a prime power solution too: $(x^2)^2 = (y^3)^5 + 1$. Even if we ask for two perfect powers whose difference is equal to some specific $t \neq 1$, solutions appear to very scarce: those shown above-right are the only ones for $t \leq 10$ when $x, y, p, q \in \{2, \ldots, 100\}$. (The diophantine equation $x^p - y^q = 6$ has no solutions in this range, indeed, I do not know if any exist at all.) In fact, a conjecture of Subbayya Sivasankaranarayana Pillai from the 1930's asserts that, for any positive integer t, there are only finitely many values of $x, y, p, q \geq 2$ solving $x^p - y^q = t$.

As with Fermat's Last Theorem, the solution to this 1844 conjecture of Eugène Catalan, was assembled over a long period of time. Victor Lebesgue quickly established that $q \neq 2$ (1850) but it then took over a hundred years before Chao Ko, in about 1960, settled the other quadratic case: $p \neq 2$, except when $x = 3$. This left p, q odd primes, and, expressing the equation as $(x - 1) \times (x^p - 1)/(x - 1) = y^q$, it could be shown that the greatest common divisor of the two left-hand factors was either 1 or p. The former case had just been eliminated by J.W.S Cassels in 1960; only 'Case II', gcd=p, remained. It was this last, formidable, hurdle that Mihăilescu surmounted. In 2000, he showed that p and q would have to be a so-called 'Wieferich pair': satisfying $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$; then, in 2002, he showed that such solutions were an impossibility.

Web link: www.ams.org/bull/2004-41-01/ (click on the article by Tauno Metsänkylä).

Further reading: *Catalan's Conjecture* by René Schoof, Springer-Verlag, London, 2008.

Created by Robin Whitty for www.theoremoftheday.org