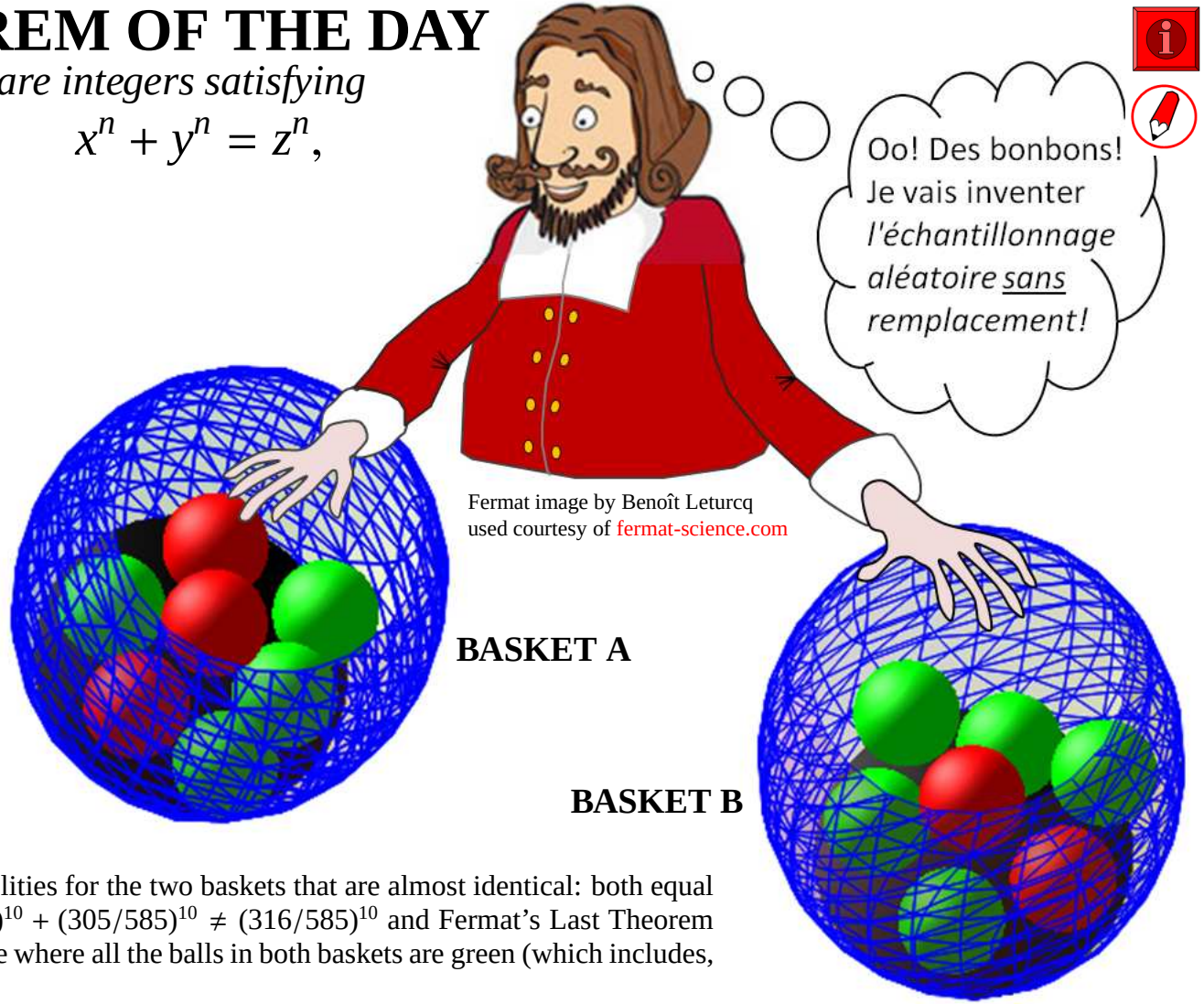
THEOREM OF THE DAY

Fermat's Last Theorem *If x, y, z and n are integers satisfying*

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

then either $n \leq 2$ or $xyz = 0$.



Fermat image by Benoît Leturcq
used courtesy of fermat-science.com

It is easy to see that we can assume that all the integers in the theorem are positive. This allows a legitimate, but totally different, way of asserting the theorem, conceived by the engineer Edward C. Molina. Unlike Fermat in the picture we are going to take balls at random with replacement. From Basket A we take one ball and then replace it. Then we take a second ball. We do the same for Basket B. The probability that both A balls are the same colour (both red or both green) is $(3/7)^2+(4/7)^2$. The probability that both B balls are green, is $5/7\times5/7$. Now the Pythagorean equality $3^2+4^2 = 5^2$ tells us that the probabilities are equal: $9/49 + 6/49 = 25/49$. What if we choose $n > 2$ balls with replacement? Can we again fill each of the baskets with N balls, red and green, so that taking n with replacement will give equal probabilities? From an experimental viewpoint we might well be satisfied by one of many Fermat 'near-misses'. For example, take $N = 10$ and put 585 balls in each basket, with 305 green balls in basket A and 316 green balls in basket B. We get probabilities for the two baskets that are almost identical: both equal to 0.0021150087, to 10 decimal places. Nevertheless, $(280/585)^{10} + (305/585)^{10} \neq (316/585)^{10}$ and Fermat's Last Theorem says we can never have equality for $n > 2$, except in the trivial case where all the balls in both baskets are green (which includes, vacuously, the possibility that $N = 0$).

Another, much more profound, way of restating Fermat's Last Theorem: if $a^n + b^n$, for $n > 2$ and positive integers a and b, is again an n-th power of an integer then the rational elliptic curve $y^2 = x(x - a^n)(x + b^n)$, known as the **Frey curve**, cannot be modular (is not a rational map of a modular curve). So it is enough to prove the **Taniyama-Shimura-Weil conjecture:** *all rational elliptic curves are modular*.

Fermat's innocent statement was famously left unproved when he died in 1665 and was the last of his unproved 'theorems' to be settled true or false, hence the name. The non-modularity of the Frey curve was established in the 1980s by the successive efforts of Gerhard Frey, Jean-Pierre Serre and Ken Ribet. The Taniyama-Shimura-Weil conjecture was at the time thought to be 'inaccessible' but the technical virtuosity (not to mention the courage and stamina) of Andrew Wiles resolved the 'semistable' case, which was enough to settle Fermat's assertion. His work was extended to a full proof of Taniyama-Shimura-Weil during the late 90s by Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor.

Web link: www-groups.dcs.st-and.ac.uk/history/HistTopics/Fermat's_last_theorem.html
Further reading: *Fermat's Last Theorem* by Simon Singh, Fourth Estate Ltd, London, 1997.