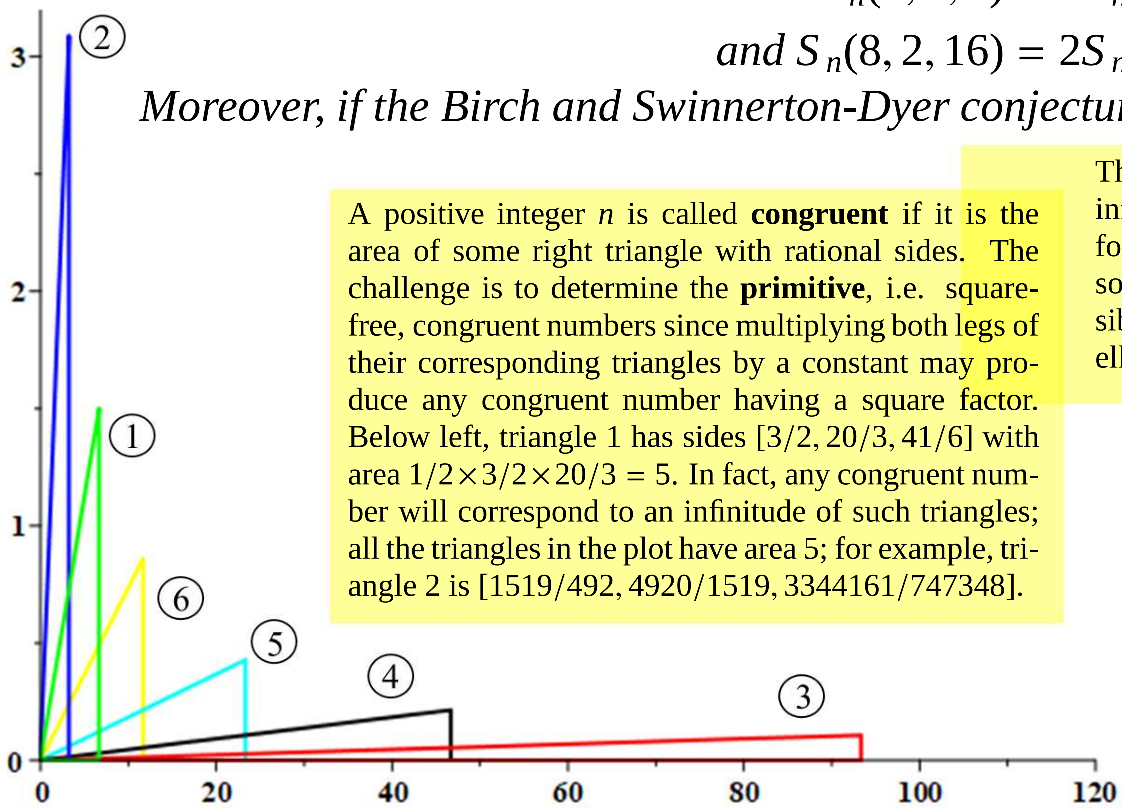
THEOREM OF THE DAY

Tunnell's Theorem *Let n be a square-free positive integer and denote by $S_n(a,b,c)$ the number of solutions in integers, x,y,z, of the equation $ax^2+by^2+cz^2=n$. Then a necessary condition for n to be a congruent number is that*

$$S_n(2,1,8) = 2S_n(2,1,32) \quad n \text{ odd}$$

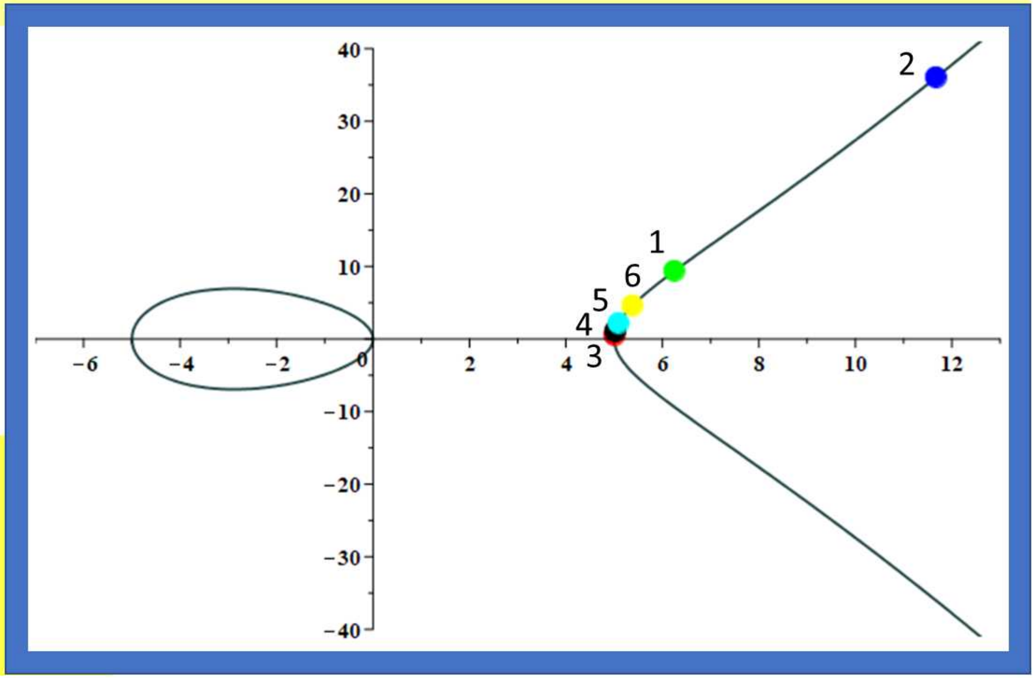
$$\text{and } S_n(8,2,16) = 2S_n(8,2,64) \quad n \text{ even}.$$

Moreover, if the Birch and Swinnerton-Dyer conjecture is true then this condition is also sufficient.



A positive integer n is called **congruent** if it is the area of some right triangle with rational sides. The challenge is to determine the **primitive**, i.e. square-free, congruent numbers since multiplying both legs of their corresponding triangles by a constant may produce any congruent number having a square factor. Below left, triangle 1 has sides $[3/2, 20/3, 41/6]$ with area $1/2\times 3/2\times 20/3 = 5$. In fact, any congruent number will correspond to an infinitude of such triangles; all the triangles in the plot have area 5; for example, triangle 2 is $[1519/492, 4920/1519, 3344161/747348]$.

The infinitude of triangles given by a congruent number n in turn corresponds to an infinitude of rational points (x,y) on the elliptic curve $y^2 = x^3 - n^2x$, depicted below for $n=5$. So determining if a number is congruent is part of a much larger challenge, solved conjecturally by Birch and Swinnerton-Dyer, to determine the structure (possibly trivial, termed 'rank zero') of the infinite set of rational points on an arbitrary elliptic curve $y^2 = x^3 + ax + b$.



The word 'congruent' comes from Fibonacci's use of the term 'congruum' to mean the common difference in a sequence of three rational squares in arithmetic progression. In another correspondence, any such sequence u^2, v^2, w^2, with common difference ns^2, gives a right triangle $(w-u)/s, (w+u)/s, 2v/s$, with area n. The sequence $(31/6)^2, (41/6)^2, (49/6)^2$, for instance, is an arithmetic progression with common difference 5×2^2, and corresponds to triangle 1 above.

Jerrold Bates Tunnell's 1983 result is based on deep progress towards Birch and Swinnerton-Dyer, notably by John Coates and Andrew Wiles and by Victor Kolyvagin. It potentially solves 'the oldest open problem in mathematics', to determine which numbers are congruent. E.g. $n=26$ cannot be congruent because $S_{26}(8,2,16) = |\{(\pm1,\pm1,\pm1),(\pm1,\pm3,0)\}| = 12 \neq 2\times S_{26}(8,2,64) = 2\times|\{(\pm1,\pm3,0)\}| = 8$.

Web link: www.pnas.org/doi/epdf/10.1073/pnas.1219394110

Further reading: *Introduction to Elliptic Curves and Modular Forms, 2nd Edition* by Neal Koblitz, Springer-Verlag, New York, 1993.