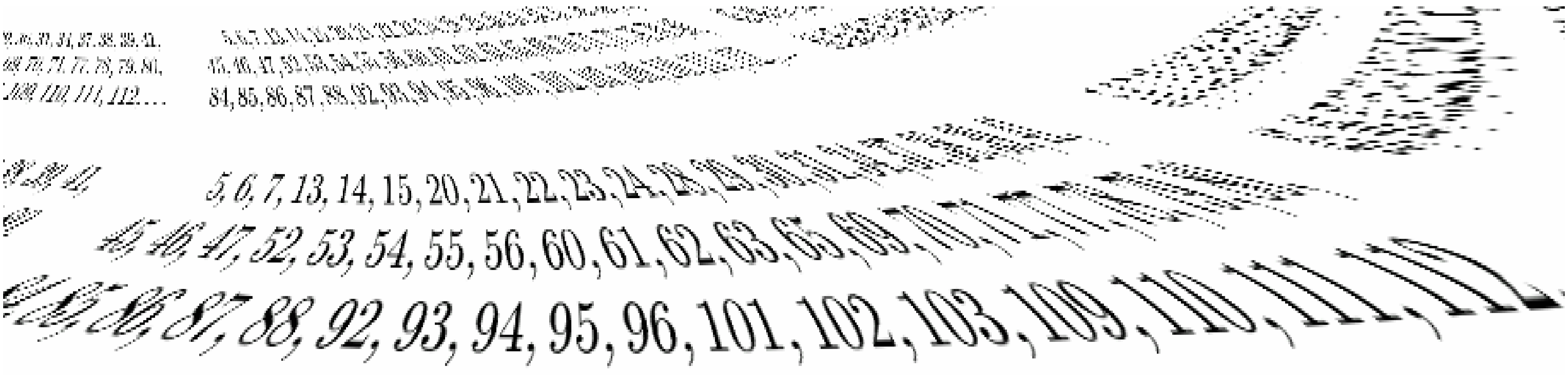
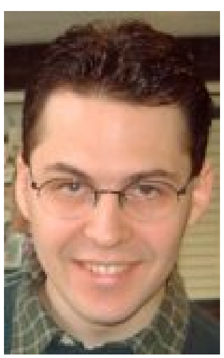
Congruent Numbers and Cubic Curves



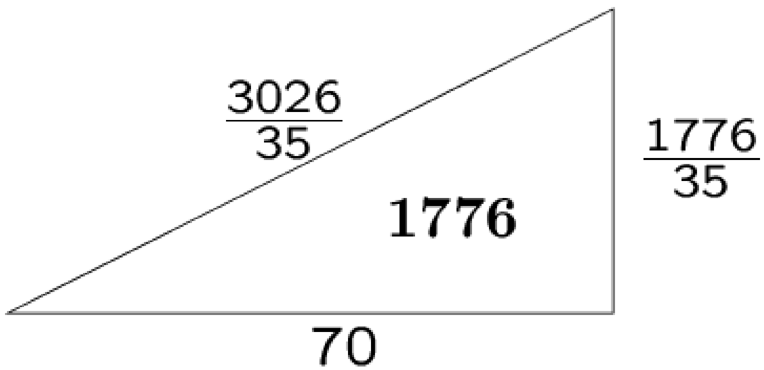
$$y^2 = x^3 - n^2 x$$



William A. Stein

http://modular.fas.harvard.edu

Some "Historical" Observations



1776 is the area of a rational right triagonal.

One can prove that 2001, on the other hand, is not the area of a right triangle!

Congruent Numbers

Definition: An integer n is called **congruent** if it is the area of a rational right triangle.

Why "congruent?" Suppose n is congruent, so there is a right triangle with side lengths *X*, *Y*, and *Z* and 1/2*XY = *n*. Let *x* = (Z/2)^2. Then *x*−*n*, *x*, and *x*+*n* are all squares, and *n* is the common *congruence*.

If we let $x = (Z/2)^2 = (3026/70)^2$, then

$$x - 1776 = \left(\frac{337}{35}\right)^2, \qquad x = \left(\frac{3026}{70}\right)^2, \qquad x + 1776 = \left(\frac{2113}{35}\right)^2.$$

Some Examples

5 is the area of the triangle with sides *X=3/2, Y=20/3, Z=41/6*

6 is the area of the triangle with sides *X=3, Y=4, Z=5*

7 is the area of the triangle with sides *X=24/5, Y=35/12, Z=337/60*

Theorem (Pierre Fermat):

The number 1 is not a congruent number.

Open Problem

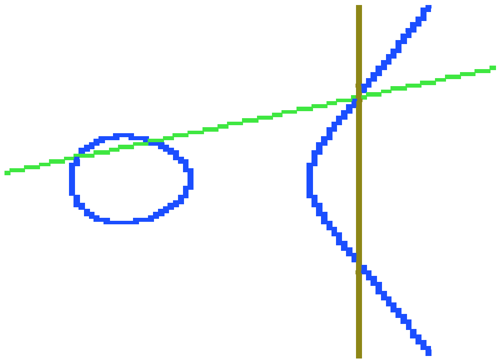
What is going on?
* Give a simple criterion to determine whether or not a number n is congruent.
* When n is congruent, give an effective algorithm to find a rational right triangle whose area is n.

These questions have been open for over a thousand years. However they are almost, but not quite, solved today. I predict that you will live to see (or find?) a complete solution!

A Connection with Cubic Equations

Theorem: *A number n is congruent if and only if the following equation has more than the three obvious solutions:*

$$y^2 = x^3 - n^2 x$$



Examples:

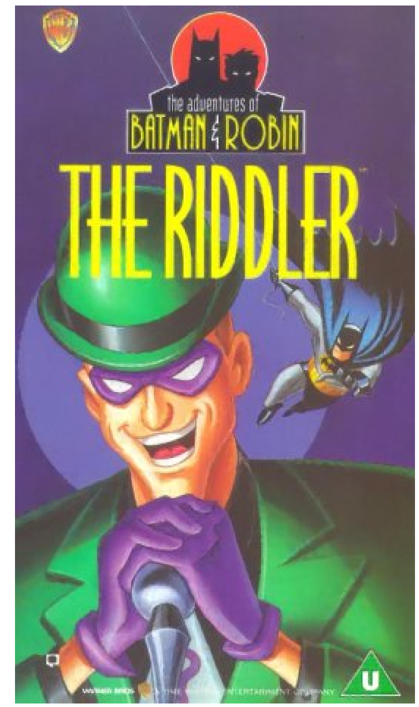
$n = 5:$ $\quad y^2 = x^3 - 25x,$ $\quad$ solution: $x = -4, \quad y = 6$

$n = 6:$ $\quad y^2 = x^3 - 36x,$ $\quad$ solution: $x = -3, \quad y = 9$

$n = 1:$ $\quad y^2 = x^3 - x,$ $\quad$ no nontrivial solutions (Fermat)

New Problem

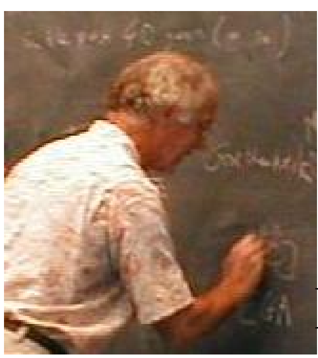
How can we possibly tell whether or not this cubic equation has lots of solutions or just the three obvious ones????



? ? ?

Two Brits, Bryan Birch and Sir Peter Swinnerton –Dyer found a conjectural answer in the 1960s.

?


Birch

?

$$y^2 = x^3 - n^2x$$?


Swinnerton–Dyer

Birch and Swinnerton-Dyer

- Their conjecture is still open! And if you solve it, the Clay Math Institute will give you a million dollars. See Wiles's paper at the Clay Math Institute's "Millenial Problems" web page.

The BSD Conjecture

An unproved special case of the BSD conjecture (Tunnell):

Let n be an odd square−free number. Then $y^2 = x^3 - n^2 x$ *has more than three solutions if and only if*

$$\#\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n\}$$
$$= 2 \cdot \#\{(a,b,c) : 2a^2 + b^2 + 32c^2 = n\}$$

(Here a, b, and c are integers.)

The BSD conjecture is a generalization of this assertion. It gives a conjectural way of telling whether or not a cubic curve has infinitely many solutions. Nobody knows how to prove even the special case given above, though there are many partial results.

Some Examples

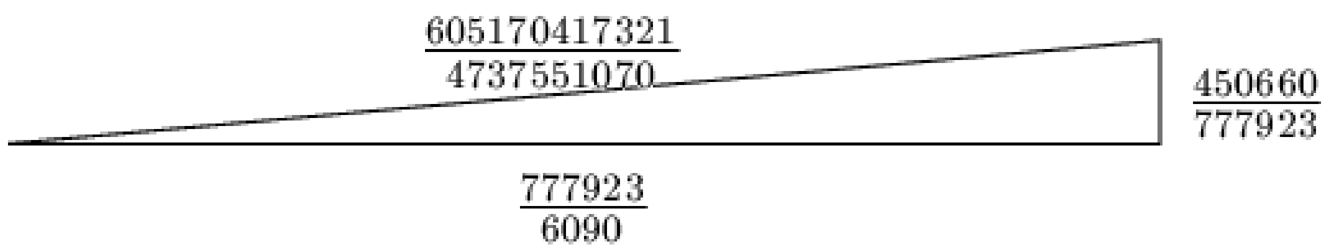
When $n=1$, there are exactly two triples in each case $(0,1,0)$ and $(0,-1,0)$. Thus the conjecture (correctly) asserts that $n=1$ is not a congruent number. *In fact, this part of the conjecture was been proved by Kolyvagin in the late 1980s if the cardinality condition fails, then n is not a congruent number.*

When $n=5$, both sets are empty. Indeed, there are lots of solutions to the cubic, as we saw.

When $n=37$, both sets are empty, so the conjecture predicts that there are interesting solutions to the cubic. We find the solution

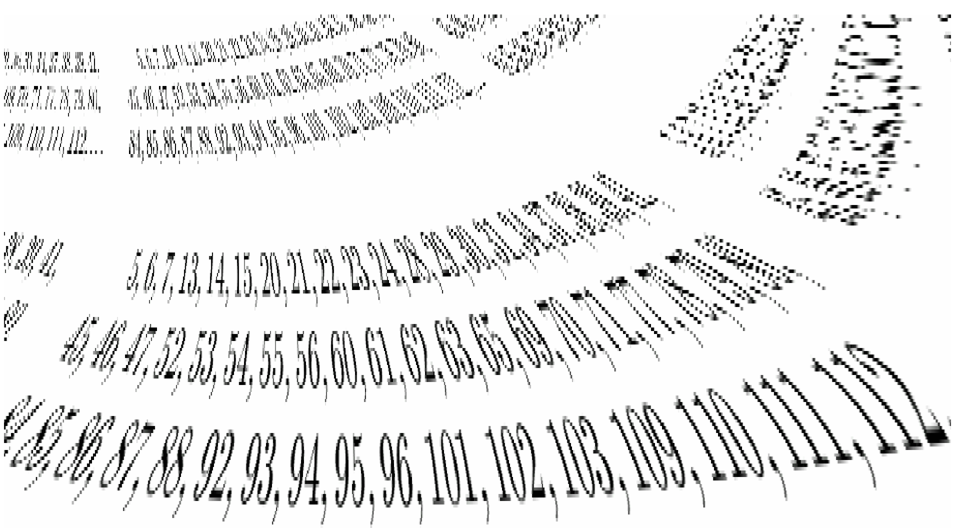
$$x = 28783225/1764, \quad y = -154421605115/74088.$$

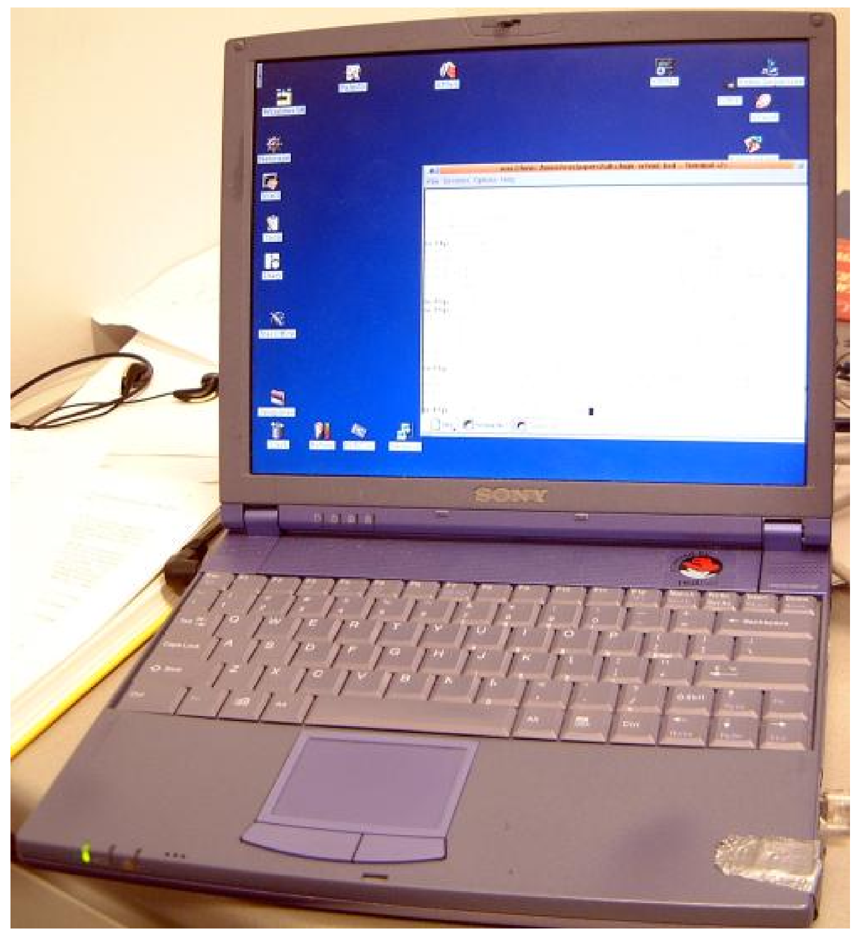
From this solution, there is a way to manufactor the following right rational triangle, whose area is $n=37$:



Let's *bravely* try some examples on my laptop!

Pick a (reasonably small) number!



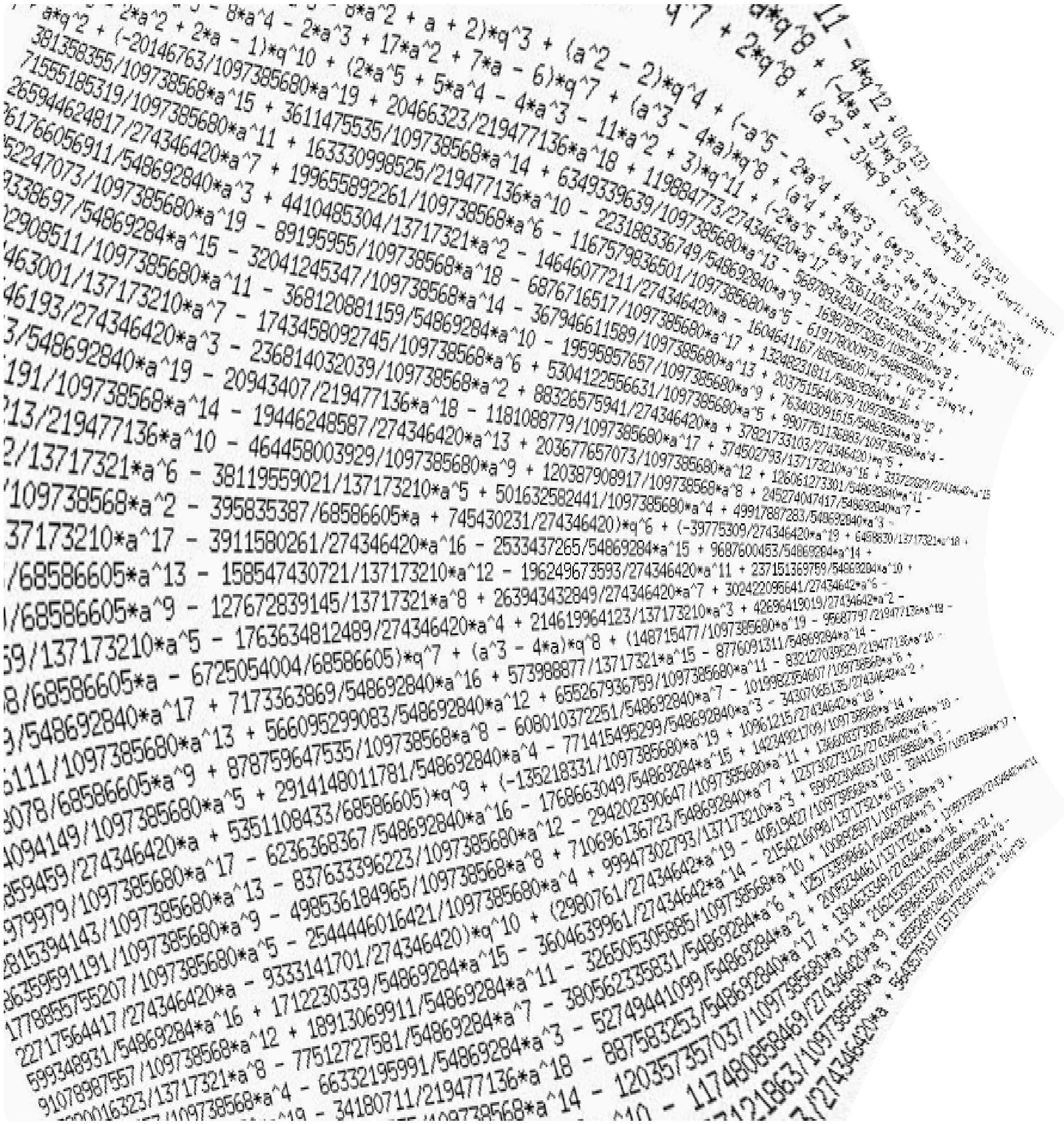


References

If you want to learn more about the congruent number problem and the Birch and Swinnerton–Dyer conjecture, I recommend the beautiful book by **Neil Koblitz**, *Introduction to Elliptic Curves and Modular Forms*.

A nice summary by **Andrew Wiles** of the Birch and Swinnerton–Dyer conjecture can be found at the Clay Math Institues web page, where one million dollars is offered for its solution.
(See http://www.claymath.org.)

Thank you for coming.



Any Questions?