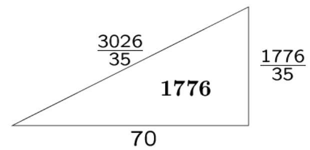
Math 124, Lecture 33

Introduction to the Congruent Number Problem

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

William A. Stein
http://modular.fas.harvard.edu

Some "Historical" Observations



1776 is the area of a rational right triagonal.

2001 is not the area of a right triangle!

Congruent Numbers

Definition: An integer n is said to be **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 Problems

* Give a usable criterion to determine whether or not a number n is congruent.

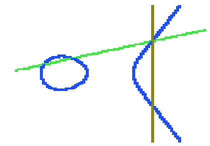
* When n is congruent, give an effective algorithm to find a rational right triangle whose area is n.

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

Proposition: *A squarefree number n is congruent if and only if the following elliptic curve has positive rank (i.e.,infinitely many rational points):*

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



Examples:

$n = 5:$	$y^2 = x^3 - 25x,$	solution: $x = -4, \quad y = 6$
$n = 6:$	$y^2 = x^3 - 36x,$	solution: $x = -3, \quad y = 9$
$n = 1:$	$y^2 = x^3 - x,$	no nontrivial solutions (Fermat)

Sketch of Proof

First suppose that n is a congruent number, so n is the area of a right triangle with side lengths X < Y<Z. Then, as mentioned above, if a = (Z/2)^2, then a−n, a, and a+n are all positive perfect squares (e.g., add X^2 + Y^2 = Z^2 to 2X*Y=4*n and factor). Thus y^2 = (x−n)x(x+n)=x^3−n^2x has a rational point with x coordinate equal to a and nonzero y−coordinate equal to the square root of the product (a−n)a(a+n).

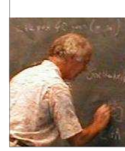
Next suppose that P is a point of infinite order on y^2 = (x−n)x(x+n). Then one can check that the x−coordinate of 2*P is the square of a rational number. Working backwards from the above, one finds X, Y, and Z. (There are many details to clarify here, that I won't clarify in class today.)

New Problem

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

? ? ?

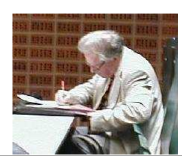
Two Brits, Bryan Birch and Sir Peter Swinnerton −Dyer found a conjectural answer in the 1960s. ?



Birch

?

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



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. Download Wiles's paper about BSD from the Math 124 web page. I will talk about it on Wednesday and Friday.

BSD and Congruent Numbers

Conjecture (Tunnell):

Let n be an odd square−free number. Then $y^2 = x^3 - n^2 x$ *has positive rank 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. There is a similar statement when n is even.)

Tunnell used modular forms in a very clever wayto prove that L(E_n,1)=0 if and only if the above equality holds. He used a deep theorem of Waldspurger that produces a modular form with the property that L(E_n,1)=0 if and only if the n−th Fourier coefficient of the form is 0. He then computes that modular form explicitly and finds that the nth coefficient is essentially the difference of the lhs and rhs in the above equality. *If the cardinalities are different than it is a theorem (of V. Kolyvagin) that n is not a congruent number.*

Some Examples

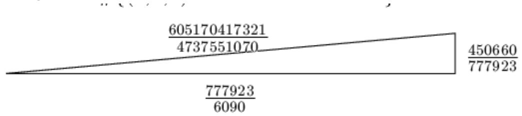
When $n=1$, *there are exactly two triples in each case (0,1,0) and (0,−1,0).* Thus the part of the conjecture that is a theorem correctly asserts that $n=1$ is not a congruent number.

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

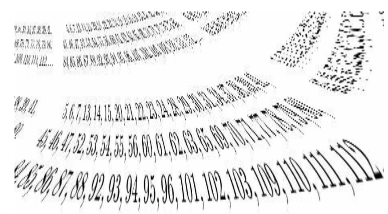
When $n=37$, both sets are empty, so the conjecture predicts that there are interesting solutions to the cubic. We find the solution

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

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



Let's try some examples!



The best place to read about the congruent number problem is in **Neil Koblitz's book**, *Introduction to Elliptic Curves and Modular Forms.*