BROWN

The Congruent Number Problem

Problems from the History of Mathematics

Lecture 12 — March 5, 2018

Brown University

Statement of the Problem

The Congruent Number Problem is a classic problem in number theory which concerns the possible areas of right triangles with rational sides. Equivalently,

The Congruent Number Problem:

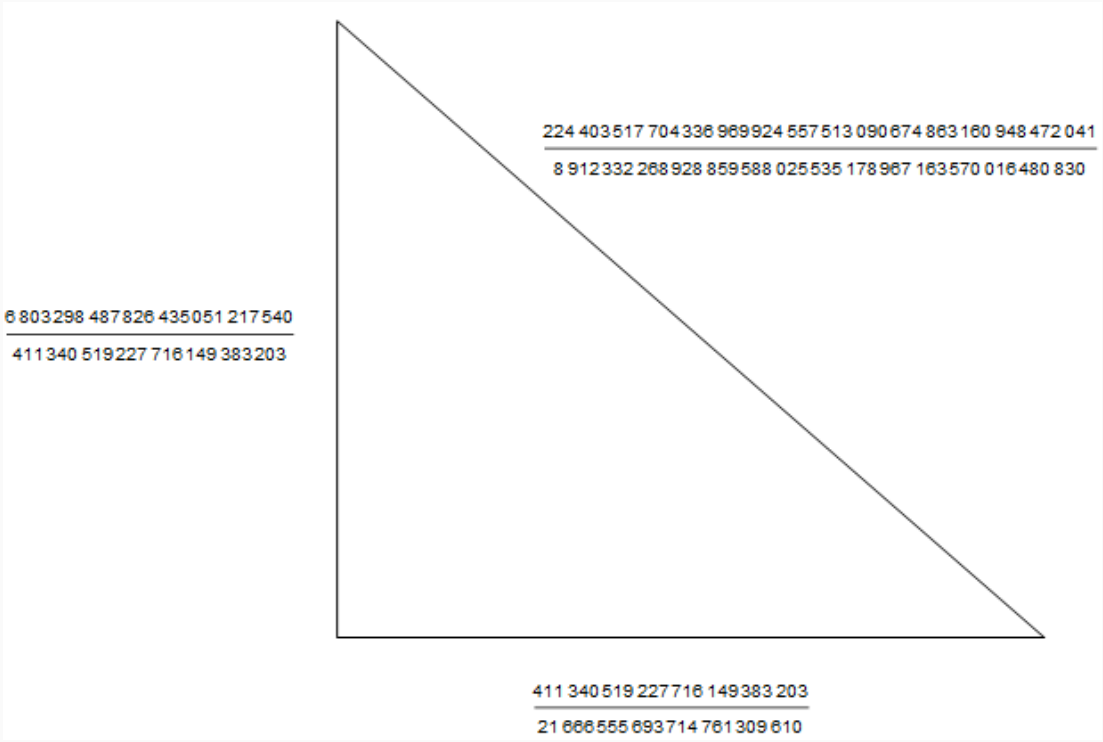
Which square-free integers arise as the areas of right triangles with rational side lengths?

Ex: The familiar $(3, 4, 5)$ triangle shows that 6 is a congruent number.

The possibility of rational side lengths complicates the search for such triangles. For example, while it might not be obvious, 5 is a congruent number. It is the area of the triangle with side lengths $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$.

A Computationally Challenging Problem

The challenge in determining whether or not an integer is congruent is best seen by example. The following triangle, found by Zagier (c. 1990), shows that 157 is a congruent number:



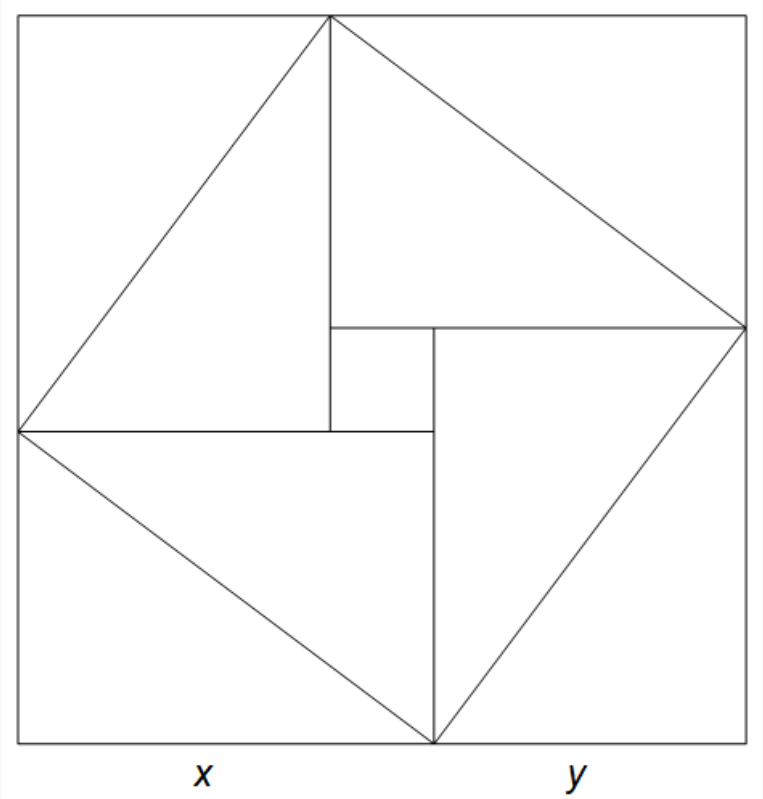
This example also begs the question of whether there exists an effective algorithm to compute such triangles.

Early History of the Congruent Number Problem

Contributions of Diophantus

Various sources credit the statement of the CNP to different authors. The oldest attribution is given to Diophantus, who found solutions to $(x_1 + x_2 + x_3 + x_4)^2 \pm x = k^2$.

Ignoring the plentitude of variables, this is the problem of finding a linear progression of three squares with common difference x. This problem is equivalent to the CNP (as illustrated at right) and Diophantus even begins his solution by constructing a triangle of area x.



The CNP in Islamic Mathematics

Diophantus' *Arithmetica* reads as a problem book and considers problems in an ad hoc manner. A more general treatment of the CNP appears for the first time in an anonymous Arab manuscript dated prior to 972.

There is no indication that the work of Diophantus appeared in the Middle East until Wafâ's translation in 988.[1]

In any case, the CNP was regarded as an important problem in Islamic mathematics by the end of the tenth century. Mohammed Ben Alhocain refers to the CNP as the "principal object in the theory of rational right triangles."[2]

---

[1] Although it is possible that knowledge of Diophantus passed to the Arabs indirectly via India.

[2] This should be taken in the context of an earlier problem concerning rational right triangles: their classification, as resolved by the time of Euclid.

The Contributions of Fermat

The Contributions of Fermat

Contributions from a great number of Islamic mathematicians led to modest lists of integers which were known to be congruent. The CNP was then brought to Europe by Fibonacci, where it was studied by the familiar names of Luca Pacioli, Tartaglia, and Cardano.

No number was shown to be *non-congruent* until the pioneering work of Pierre de Fermat (c. 1607-1665), who proved the following:

Theorem (Fermat's Right Triangle Theorem):

If three squares form an arithmetic progression, then the gap between consecutive numbers cannot also be square. Thus 1 is not congruent.

This result is Fermat's **only** complete proof.[3] It uses Fermat's method of infinite descent, a powerful tool in non-existence proofs which uses a single 'large' solution to construct ever smaller ones.[4]

[3] It was written in his copy of Diophantus and published posthumously.

[4] It's the contrapositive of induction.

Infinite Descent

The following is a typical example of infinite descent:

Ex: Prove that $x^2 + y^2 = 3z^2$ has no positive integer solutions

Proof: Suppose that (x, y, z) is a solution. We must have $3 \mid (x^2 + y^2)$. Since the only quadratic residues in $\mathbb{Z}/3\mathbb{Z}$ are $\{0, 1\}$, $x^2 + y^2 \equiv 0 \mod 3$ only when $x \equiv y \equiv 0 \mod 3$.

Then $x^2 + y^2$ is divisible by 9, so $3 \mid z$ as well. The solution $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ is then integral and smaller, which gives a contradiction by descent. $\square$

Fermat's Right Triangle Theorem

After this warm-up, let's prove Fermat's Right Triangle Theorem:

Proof: Suppose that x, y, z are the integer sides of a right triangle with square area. WLOG, we assume that this triangle is primitive and thus

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2$$

by Euclid. This triangle has area $mn(m^2 - n^2)$, which we assume is a square. Since m, n, $m - n$, and $m + n$ are relatively prime, each is a square. Let $m = s^2$, $n = t^2$, $m + n = u^2$, and $m - n = v^2$.

Since m, n have different parity, u, v are both odd. Then $u + v$ and $u - v$ are both even. Consider the right triangle with side lengths

$$(\tfrac{u-v}{2}, \tfrac{u+v}{2}, \sqrt{\tfrac{(u-v)^2}{4} + \tfrac{(u+v)^2}{4}}) = (\tfrac{u-v}{2}, \tfrac{u+v}{2}, s).$$

The area is $\frac{1}{8}(u^2 - v^2) = m/4$, which gives a new right triangle with integer sides[5] and a smaller area. □

[5] Since $u + v$ and $u - v$ are both even and one is divisible by 4.

Modern Developments

A Connection to Elliptic Curves

Suppose that $a^2 + b^2 = c^2$ and that $ab/2 = n$ (with n a parameter). These two equations describe surfaces in $\mathbb{R}^3$, so we expect them to intersect in a curve.

To describe this curve, let $c = t + a$. Then $a^2 + b^2 = (t + a)^2$, ie. $2at = b^2 - t^2$. Substitute $a = 2n/b$ and multiply by bn^3/t^3 to get

$$\frac{4n^4}{t^2} = \left(\frac{bn}{t}\right)^3 - n^2\frac{bn}{t}.$$

Now let $y = 2n^2/t$ and $x = bn/t$, to obtain the elliptic curve

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

Rational points on this elliptic curve (with $y \neq 0$) correspond to triangles with area n. For example, the solution $36^2 = 12^2 - 36 \cdot 12$ represents the fact that 6 is congruent.

Tunnell's Conditional Proof

The connection between congruent numbers and elliptic curves was fully appreciated by Jerrold Tunnell in 1983, when he proved the following:

Tunnell's Theorem:

Let n be square-free and odd and consider the sets

$$A_n = \{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}$$
$$B_n = \{(x, y, z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\}.$$

If n is congruent, then $2\#A_n = \#B_n$. The converse holds under the Birch–Swinnerton-Dyer Conjecture. (A similar statement exists for even n.)

BSD is listed as one of the seven Clay Millennium Problems and remains open to this day.

Questions?