Congruent number problem

—A thousand year old problem

Maosheng Xiong

Department of Mathematics,
Hong Kong University of Science and Technology

Original version

Mohammed Ben Alhocain, in an Arab manuscript[1], written before 972, wrote the following:
The principal object of the theory of rational right triangles is to find a square that when increased or diminished by a certain number, n becomes a square.

Congruent number problem (Original version)

Given an integer n, find a (rational) square γ^2 *such that* $\gamma^2 \pm n$ *are both (rational) squares.*

[1] Dickson LE (1971) *History of the Theory of Numbers*, Vol 2, Chap 16.

Congruent number problem

Definition (Original version)

An integer n is called a congruent number if there exist rational numbers γ, a, b such that

$$\gamma^2 + n = a^2, \quad \gamma^2 - n = b^2.$$

Examples:

- 24 is a congruent:

$$5^2 + 24 = 7^2, \quad 5^2 - 24 = 1^2.$$

- so is 6:

$$\left(\frac{5}{2}\right)^2 + 6 = \left(\frac{7}{2}\right)^2, \quad \left(\frac{5}{2}\right)^2 - 6 = \left(\frac{1}{2}\right)^2.$$

It suffices to assume that n has no square factors.

History of Congruent number problem

In 1220's, Leonard Pissano was challenged by Emperor's scholars to show that 5,7 are congruent numbers:

$$5: \quad \left(\frac{49}{12}\right)^2, \quad \left(\frac{41}{12}\right)^2, \quad \left(\frac{31}{12}\right)^2$$

$$7: \quad \left(\frac{463}{120}\right)^2, \quad \left(\frac{337}{120}\right)^2, \quad \left(\frac{113}{120}\right)^2$$

Conjecture (Fibonacci)

1 is not a congruent number.

400 years later, Fermat proved this conjecture by his method of *infinite descent*.

Triangular version

Congruent number problem (Triangular version)

Given a positive integer n, find a right angled triangle with rational sides and area n.

Definition (Triangular version)

A positive integer n is called a congruent number if there exist positive rational numbers a, b, c such that

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}.$$

This was considered as a principle object of the theory of rational triangles in 10th century.

Equivalence of the two forms

Given a positive integer n, if α, β, γ are positive rational numbers such that

$$\alpha^2 = \gamma^2 - n, \quad \beta^2 = \gamma^2 + n.$$

Then

$$(\beta - \alpha)^2 + (\beta + \alpha)^2 = 2(\beta^2 + \alpha^2) = (2\gamma)^2,$$

We have the following right triangle with area n:

$$a = \beta - \alpha, \quad b = \beta + \alpha, \quad c = 2\gamma.$$

Equivalence of the two forms

Conversely, given a rational right triangle (a, b, c) with area n, that is,

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}.$$

Then

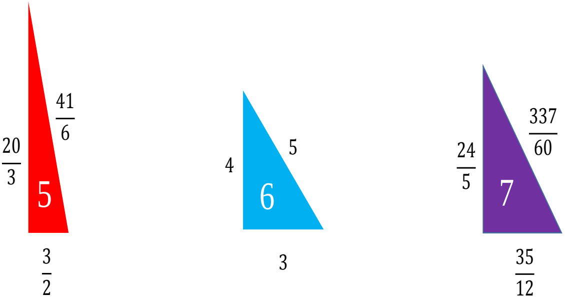
$$\left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n,$$

and

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n,$$

so that $\gamma = \frac{c}{2}$, and $\gamma^2 \pm n$ are both rational squares.

5,6,7 are congruent numbers



Congruent primes

Theorem (Zagier)

157 is a congruent number with a precise triangle:

$$157 = \frac{ab}{2}, \quad a^2 + b^2 = c^2,$$

where

$$a = \frac{411340519227716149383203}{21666555693714761309610},$$

$$b = \frac{6803298487826435051217540}{411340519227716149383203},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Fermat's infinite descent

Theorem (Euclid's formula (300 BC))

Given (a, b, c) positive integers, pairwise coprime, and $a^2 + b^2 = c^2$ (such (a, b, c) is called a primitive Pythagorean triple). Then there is a pair of coprime positive integers (p, q) with $p + q$ odd, such that

$$a = 2pq, \quad b = p^2 - q^2, \quad c = p^2 + q^2.$$

Thus we have a Congruent number generating formula:

$$n = pq(p + q)(p - q)/\Box.$$

Example of congruent numbers

- $(p, q) = (2, 1), \quad pq(p^2 - q^2) = 2 \cdot 3, \quad n(2, 1) = 6;$
- $(p, q) = (5, 4), \quad pq(p^2 - q^2) = 5 \cdot 4 \cdot 9, \quad n(5, 4) = 5;$
- $(p, q) = (16, 9), \quad pq(p^2 - q^2) = 16 \cdot 9 \cdot 7, \quad n(16, 9) = 7;$

So 5, 6 and 7 are congruent numbers.

Infinite descent

Theorem (Fermat)

1,2,3 are non-congruent.

Proof: (for 1 being a non-congruent number)

1. Suppose 1 is congruent. Then there is an integral right triangle with minimum area: $\square = pq(p+q)(p-q)$.
2. As all 4 factors are co-prime,

$$p = x^2, \quad q = y^2, \quad p+q = u^2, \quad p-q = v^2.$$

3. Thus we have an equation with the solution as follows:

$$(u+v)^2 + (u-v)^2 = (2x)^2.$$

4. Then $(u+v, u-v, 2x)$ forms a right triangle and with a smaller area y^2. Contradiction!

Fermat 1659

In a letter to his friend, Fermat wrote:
"I discovered at least a most singular method... which I call the infinite descent. At first I used it only to prove negative assertions such as ... there is no right angled triangle in numbers whose area is a square, ... If the area of such a triangle were a square, then there would also be a smaller one with the same property, and so on, which is impossible, ..."

He adds that to explain how his method works would make his discourse too long, hence omitting the proof.

"Fortunately, just for once he (Fermat) had found room for this mystery in the margin of the very last proposition of Diophantus". – quote of Andrew Weil

Infinite descent

Fermat noted that his proof that 1 is not a congruent number also implies that there are no rational numbers x and y with $xy \neq 0$ such that $x^4 + y^4 = 1$. This led him to his claim

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.".

Fermat's claim (Fermat's last theorem) that for any integer $n \geq 3$, there are no rational numbers x and y with $xy \neq 0$ such that $x^n + y^n = 1$, was only proved by Andrew Wiles in 1994, by the development of the theory of elliptic curves.

Congruent numbers

Definition (Triangular version)

A positive integer n is called a congruent number if there exist positive rational numbers a, b, c such that

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}.$$

n is a congruent number $\iff n \cdot \square$ is a congruent number.

Theorem (Euclid's formula (300 BC))

Given (a, b, c) positive integers, pairwise coprime, and $a^2 + b^2 = c^2$ (such (a, b, c) is called a primitive Pythagorian triple). Then there is a pair of coprime positive integers (p, q) with $p + q$ odd, such that

$$a = 2pq, \quad b = p^2 - q^2, \quad c = p^2 + q^2.$$

Thus we have a Congruent number generating formula:

$$n = \frac{ab}{2} = pq(p^2 - q^2)/\Box.$$

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n : \quad ny^2 = x^3 - x.$$

Congruent number problem

If n is a congruent number, then

$$n = pq(p^2 - q^2)/\square$$

for some positive integers p, q. For the elliptic curve

$$E_n : \quad ny^2 = x^3 - x,$$

let $x = \frac{p}{q}$, we have

$$ny^2 = x^3 - x = \frac{p^3}{q^3} - \frac{p}{q} = \frac{pq(p^2 - q^2)}{q^4} = \frac{n\square}{q^4}.$$

Thus $x = \frac{p}{q}, y = \frac{\sqrt{\square}}{q^2} \neq 0$ is a rational point of E_n.

Congruent number problem

If the elliptic curve

$$E_n : \quad ny^2 = x^3 - x$$

has a rational point (x, y) with $y \neq 0$. Let $x = \frac{p}{q}$ with $\gcd(p, q) = 1$, then we have

$$ny^2 = x^3 - x = \frac{p^3}{q^3} - \frac{p}{q} = \frac{pq(p^2 - q^2)}{q^4}.$$

We see that

$$n = \frac{pq(p^2 - q^2)}{\square},$$

hence n is a congruent number.

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n : \quad ny^2 = x^3 - x.$$

A positive integer n is called a congruent number of E_n has a rational point (x, y) with $y \neq 0$. This is equivalent to the triangle version:

$$x = \frac{p}{q} \Longleftrightarrow (a, b, c) = \left(2pq, p^2 - q^2, p^2 + q^2\right).$$

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n : \quad ny^2 = x^3 - x.$$

A positive integer n is called a congruent number of E_n has a rational point (x, y) with $y \neq 0$. This is equivalent to the triangle version:

$$x = \frac{p}{q} \Longleftrightarrow (a, b, c) = \left(2pq, p^2 - q^2, p^2 + q^2\right).$$

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n : \quad ny^2 = x^3 - x.$$

A positive integer n is called a congruent number of E_n has a rational point (x, y) with $y \neq 0$. This is equivalent to the triangle version:

$$x = \frac{p}{q} \Longleftrightarrow (a, b, c) = \left(2pq, p^2 - q^2, p^2 + q^2\right).$$

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n: \quad ny^2 = x^3 - x.$$

A positive integer n is called a congruent number of E_n has a rational point (x, y) with $y \neq 0$. This is equivalent to the triangle version:

$$x = \frac{p}{q} \Longleftrightarrow (a, b, c) = \left(2pq, p^2 - q^2, p^2 + q^2\right).$$

Congruent number problem

Congruent number problem (Elliptic curve version)

For a positive integer n, find a rational point (x, y) with $y \neq 0$ on the elliptic curve:

$$E_n : \quad ny^2 = x^3 - x.$$

A positive integer n is called a congruent number of E_n has a rational point (x, y) with $y \neq 0$. This is equivalent to the triangle version:

$$x = \frac{p}{q} \Longleftrightarrow (a, b, c) = \left(2pq, p^2 - q^2, p^2 + q^2\right).$$