Congruent number problem

—A thousand year old problem

Maosheng Xiong

Department of Mathematics,
Hong Kong University of Science and Technology

A numerical example

$$E: \quad y^2 = x^3 - 5x + 8.$$

The point $P = (1,2)$ is on the curve $E(\mathbb{Q})$. To compute $2P = P + P$, take derivative on both sides of $y^2 = x^3 - 5x + 8$ we have

$$2yy' = 3x^2 - 5 \Longrightarrow y' = \frac{3x^2 - 5}{2y}.$$

So the slope of the tangent line to the elliptic curve at $P = (1,2)$ (evaluating y' for $x = 1, y = 2$) is $-\frac{1}{2}$. Thus the tangent line is

$$L: \quad y - 2 = -\frac{1}{2}(x - 1) \Longrightarrow x = -2y + 5$$

A numerical example

$$E: \quad y^2 = x^3 - 5x + 8.$$

$$L: \quad x = -2y + 5 \quad \text{(the tangent line)}$$

The point $P = (1, 2)$ is on the curve $E(\mathbb{Q})$.
Combining the two equations L and E we have

$$y^2 = (-2y + 5)^3 - 5(-2y + 5) + 8,$$

that is,

$$y^3 - \frac{59}{8}y^2 + \frac{140}{8}y - \frac{108}{8} = 0.$$

This cubic equation has three solutions $y_1 = y_2 = 2$ and y_3, satisfying

$$y_1 + y_2 + y_3 = \frac{59}{8} \Longrightarrow y_3 = \frac{27}{8}.$$

So the x-coordinate of the point is $x_3 = -2y_3 + 5 = -\frac{7}{4}$.

A numerical example

We find the extra rational point

$$x_3 = -\frac{7}{4}, y_3 = \frac{27}{8}.$$

Then

$$2P = P + P = \left(-\frac{7}{4}, -\frac{27}{8}\right).$$

A numerical example

$$E: \quad y^2 = x^3 - 5x + 8.$$

Let

$$Q = \left(-\frac{7}{4}, -\frac{27}{8}\right).$$

Using the secant line construction, similarly we find that

$$3P = P + Q = \left(\frac{553}{121}, -\frac{11950}{1331}\right).$$

Similarly,

$$4P = \left(\frac{45313}{11664}, -\frac{8655103}{1259712}\right).$$

Heron's theorem

Theorem (Heron of Alexandria, 2000 years ago)

The area n of a triangle with three sides $a, b, c > 0$ is given by

$$n^2 = s(s-a)(s-b)(s-c)$$

where $s = \frac{a+b+c}{2}$.

Heron triangle

Definition (Heron of Alexandria, 2000 years ago)

A triangle with rational sides and rational area is called a Heron triangle.

- Heron observed that $a = 13, b = 14, c = 15$ is a triangle with area $n = 84$, so 84 is the area of a Heron triangle.
- A generalized congruent number problem is to ask if n is the area of a Heron triangle with a certain angle.

Heron triangle

Definition (Heron of Alexandria, 2000 years ago)

A triangle with rational sides and rational area is called a Heron triangle.

A rational number n occurs as the area of a Heron triangle if and only if there are positive rational numbers a, b, c and a real number $\theta \in (0, \pi)$ such that

$$a^2 = b^2 + c^2 - 2bc\cos\theta, \quad \text{and } 2n = bc\sin\theta.$$

The equations imply that $(\cos\theta, \sin\theta)$ must be a rational point $\neq (\pm 1, 0)$ on the upper half of the unit circle $x^2 + y^2 = 1$. Since all rational points of the unit circle can be parameterized by $t \in \mathbb{Q}$, there is a rational number $t > 0$ such that

$$\sin\theta = \frac{2t}{t^2+1}, \quad \cos\theta = \frac{t^2-1}{t^2+1}.$$

t-congruent number

Definition

Fix a positive rational number t. A rational number n is called t-congruent if there are positive rational numbers a, b, c such that

$$a^2 = b^2 + c^2 - 2bc\frac{t^2-1}{t^2+1}, \quad \text{and } 2n = bc\frac{2t}{t^2+1}.$$

- A rational number n is t-congruent if n occurs as the area of a Heron triangle with given angle θ where

$$\sin\theta = \frac{2t}{t^2+1}, \quad \cos\theta = \frac{t^2-1}{t^2+1}.$$

- The case $t = 1$ (thus $\theta = \frac{\pi}{2}$) corresponds to the congruent number problem.

t-congruent number

Theorem

Fix a positive rational number t. Then n is a t-congruent number if and only if the following:

(i) *Either both n/t and t^2+1 are nonzero rational squares,*

(ii) *or the elliptic curve*

$$C_{n,t}: \quad y^2 = x(x-n/t)(x+nt)$$

has a rational point (x, y) with $y \neq 0$.

This will be an exercise.

The congruent number problem

Hint: For the congruent number problem, from the equations

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

How shall we find a rational point (x, y) on $E : ny^2 = x^3 - x$?
You may use the following idea: take $c = a + t$, then $a^2 + b^2 = c^2$ implies that

$$2at = b^2 - t^2.$$

Multiplying b on both sides, using $ab = 2n$, we find

$$4nt = b^3 - bt^2.$$

The congruent number problem

Diving t^3 on both sides of the previous equation, noting that $t = c - a \neq 0$, we obtain

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

Thus the point (x, y) with $x = \frac{b}{t}, y = \frac{2}{t}$ is on the elliptic curve

$$ny^2 = x^3 - x.$$

You may use this idea to prove the theorem on the relation between t congruent numbers and the corresponding elliptic curves.

t-congruent number

Theorem

Any square-free positive integer n is a t-congruent number for some positive rational number t.

Proof For any $r \in \mathbb{Q}_{>0}$ with $r \neq 1$, the rational triangle with three sides $(2, |r - r^{-1}|, r + r^{-1})$ is a right triangle with area $|r - r^{-1}|$. Hence for any n, the idea is to choose appropriate $r, s \in \mathbb{Q}_{>0}$ with $r, s \neq 1$ and to glue the rational two right triangles $(2, |r - r^{-1}|, r + r^{-1})$ and $(2, |s - s^{-1}|, s + s^{-1})$ along the side of 2, to obtain a Heron triangle with area $|r - r^{-1}| + |s - s^{-1}|$, which is hopefully $n \cdot \square$. It turns out we can take (assuming that $n > 6$)

$$r = \frac{2n}{n-1}, \quad s = \frac{n-2}{4},$$

then the total area is $\frac{(n+2)^2}{4n}$ which works.