Congruent Numbers and Elliptic Curves

Pan Yan
pyan@okstate.edu

September 30, 2014

1 Problem

In an Arab manuscript of the 10th century, a mathematician stated that the principal object of rational right triangles is the following question[2].

Congruent number problem (Original version). Given a positive integer n, find a rational square a^2 ($a \in \mathbb{Q}^*$) such that $a^2 \pm n$ are both rational squares.

Definition 1.1. An integer n is a *congruent number* if there exists a rational square a^2 such that $a^2 \pm n$ are both rational squares.

Example 1.2. (i) 5 is a congruent number:

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2, \left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2.$$

(ii) 6 is a congruent number:

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

(iii) 7 is a congruent number:

$$\left(\frac{337}{120}\right)^2 - 7 = \left(\frac{113}{120}\right)^2, \left(\frac{337}{120}\right)^2 + 7 = \left(\frac{463}{120}\right)^2.$$

Definition 1.3. A right triangle is *rational* if its legs and hypotenuse are all rational numbers.

Congruent number problem (Triangular version). Given a positive integer n, find a right triangle such that its sides are rational and its area equals n.

Proof of the equivalence of the two versions. (Origional version $\Rightarrow$ Triangular version) Suppose $\alpha^2, \beta^2, \gamma^2$ are arithmetic progression of rational squares with common difference n. Then the right angled triangle with legs and hypotenuse

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

has an area of n.

(Triangular version $\Rightarrow$ Origional version) Conversely, suppose we have a rational right triangle $[a, b, c]$ with area n. Then $\left(\frac{a-b}{2}\right)^2, \left(\frac{c}{2}\right)^2, \left(\frac{a+b}{2}\right)^2$ is an 3-term arithmetic progression with common difference n. □

Example 1.4. (i) 5 is the area of rational right angled triangle $[\frac{20}{3}, \frac{3}{2}, \frac{41}{6}]$.

(ii) 6 is the area of rational right angled triangle $[3, 4, 5]$.

(iii) 7 is the area of rational right angled triangle $[\frac{24}{5}, \frac{35}{12}, \frac{337}{60}]$.

Remark 1.5. *We assume n is a square free positive integer, because if $[a, b, c]$ is a right angled triangle with area n, then $[as, bs, cs]$ is also a right angled triangle with area ns^2.*

Open Problem:

(i) Give a simple criterion to determine whether or not a number n is congruent.

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

Theorem 1.6 (Fermat)**.** *1, 2, 3 are not congruent numbers.*

Proof. We use Fermat's Infinite Decent Method to prove 1 is not congruent number. His argument based on Euclidean formula: Given (a, b, c) positive integers, pairwise coprime, and $a^2 + b^2 = c^2$. Then there is a pair of coprime positive integer (p, q) with $p + q$ odd such that

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

Thus we have a congruent number generating formula:

$$n = pq(p + q)(p - q)/m^2. \tag{1.1}$$

Step 1: Suppose 1 is congruent number, then there is an integral right angled triangle $[a, b, c]$ with minimum area $m^2 = pq(p + q)(p - q)$.

Step 2: Since all 4 factors of m^2 are coprime,

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

Step 3: We have an equation

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

Step 4: $(u + v, u - v, 2x)$ forms a right angled triangle with a smaller area y^2. This is a contradiction. □

Corollary 1.7 (Fermat's Right Triangle Theorem)**.** *If n is a square, then n is not a congruent number.*

Remark 1.8. *Although we have formula (1.1) to generate congruent numbers, this algorithm is far from efficient. For example, $n = 157$ is the area of the rational right angled triangle with the following legs and hypotenuse (due to Zagier):*

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

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

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

Mathematicians can not be replaced by computers!

2 Elliptic Curves

Connection with Elliptic Curves

Theorem 2.1. *For $n > 0$, there is a one-to-one correspondence between the following two sets:*

$$\{(a,b,c) : a^2 + b^2 = c^2, \frac{1}{2}ab = n\}, \ \{(x,y) : y^2 = x^3 - n^2x, y \neq 0\}.$$

Mutually inverse correspondences between these two sets are

$$(a,b,c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \ (x,y) \mapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

Fix a real number $n \neq 0$. The real solutions (a,b,c) to each of the following equations

$$a^2 + b^2 = c^2, \frac{1}{2}ab = n, \tag{2.1}$$

describe a surface in $\mathbb{R}^3$. So it is natural to expect these two surfaces to intersect in a curve. We want to describe such a curve, which will be $y^2 = x^3 - n^2x$ under the right choice of coordinates.

Let $c = t + a$, substitute it into $a^2 + b^2 = c^2$, we get $b^2 = t^2 + 2at$, or equivalently,

$$2at = b^2 - t^2. \tag{2.2}$$

Since $ab = 2n \neq 0$, neither a nor b is 0, so we can write $a = \frac{2n}{b}$ and substitute it into (2.2):

$$\frac{4nt}{b} = b^2 - t^2.$$

Multiplying each side by b, we get

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

Dividing by t^3 ($t \neq 0$, otherwise $a = c$ and then $b = 0$, but $ab = 2n \neq 0$) yields

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

Multiplying each side by n^3, we get

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

Set $x = \frac{nb}{t} = \frac{nb}{c-a}$ and $y = \frac{2n^2}{t} = \frac{2n^2}{c-a} \neq 0$, so $y^2 = x^3 - n^2 x$.

Remark 2.2. *(i) The equation $y^2 = x^3 - n^2 x$ has three trivial rational solutions with $y = 0$: $(0,0), (n,0), (-n,0)$.*

(ii) The correspondence preserves positivity.

(iii) The equation $y^2 = x^3 - n^2 x$ is an elliptic curve!

Congruent number problem (Elliptic Curve version). For a positive number n, find a rational point with $y \neq 0$ on the elliptic curve $E_n : y^2 = x^3 - n^2 x$.

The viewpoint of the equation $y^2 = x^3 - n^2 x$ allows one to do something striking: produce a new rational right angled triangle with area n from two known triangles (by the group law of points on elliptic curves).

Theorem 2.3 (Mordell, 1922)**.** $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$.

Theorem 2.4 (Lutz-Nagell Theorem, 1937, 1935)**.** *For an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$ and let $D = -(4A^3 + 27B^2) \neq 0$. If (x, y) is a torsion point, then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 | D$.*

In the case of $E_n : y^2 = x^3 - n^2 x$, $D = 4n^6$. So the torsion points are either $y = 0$ or $y^2 | 4n^6$. But $y^2 = x^3 - n^2 x$ has no solution with $y \neq 0, x, y \in \mathbb{Z}$, and $y^2 | 4n^6$. Hence, we have the following theorem.

Theorem 2.5.

$$E_n(\mathbb{Q})_{tors} = \{O, (0,0), (n,0), (-n,0)\}.$$

Remark 2.6. *If there is one nontrivial rational point on the elliptic curve $E_n : y^2 = x^3 - n^2 x$, then there are infinitely many rational points on the elliptic curve $E_n : y^2 = x^3 - n^2 x$. The argument is as following. Suppose $P = (x, y)$ with $y \neq 0$ is a rational point on the elliptic curve. Then P can not be a torsion, so $nP \neq O$ if $n \in \mathbb{Z}$ and $n \neq 0$. This means that $P, 2P, 3P, \cdots$ are all distinct. If not, then $nP = mP$ for some $n < m$ and then $O = mP - nP = (m - n)P$, contradiction.*

Theorem 2.7. *A positive integer n is a congruent number if and only if the elliptic curve $E_n : y^2 = x^3 - n^2x$ over $\mathbb{Q}$ has rank greater than 0.*

Remark 2.8. *Any point with $y \neq 0$ gives rank > 0.*

Theorem 2.9. *A positive integer n is a congruent number if and only if there exists a point of infinite order on the elliptic curve $E_n : y^2 = x^3 - n^2x$.*

Criterions for Non-Congruent Numbers and Conditions for Congruent Numbers

Moreover, the viewpoint of thinking about congruent numbers in terms of the elliptic curve $y^2 = x^3 - n^2x$ goes far beyond the construction of new rational right angled triangle with area n. This viewpoint leads to a tentative solution to the whole congruent number problem! In 1983, Tunnell used arithmetic property of the elliptic curve $E_n : y^2 = x^3 - n^2x$ to discover a previously unknown elementary necessary condition on congruent numbers and he was able to prove the condition is also sufficient if the weak Birch and Swinnerton-Dyer conjecture is true.

Theorem 2.10 (Tunnell, 1983)**.** *Let n be an squarefree positive integer. Set*

$$a(n) = \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n\},$$

$$b(n) = \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 32z^2 = n\},$$

$$a'(n) = \#\{(x, y, z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 16z^2 = n\},$$

$$b'(n) = \#\{(x, y, z) \in \mathbb{Z}^3 : 8x^2 + 2y^2 + 64z^2 = n\}.$$

For odd n, if n is a congruent number, then $a(n) = 2b(n)$; for even n, if if n is a congruent number, then $a'(n) = 2b'(n)$. Moreover, if the weak Birch and Swinnerton-Dyer conjecture is true for the elliptic curve $E_n : y^2 = x^3 - n^2x$, then the conditions are also sufficient.

Remark 2.11. *Tunnell's theorem provides an unconditional method of proving a squarefree integer n is not congruent, and a conditional method of proving a squarefree integer n is congruent.*

(i) If n is odd, and $a(n) \neq 2b(n)$, then n is not a congruent number. If n is even, and $a'(n) \neq 2b'(n)$, then n is not a congruent number.

(ii) Suppose the weak BSD conjecture is true for the elliptic curve $E_n : y^2 = x^3 - n^2x$. If n is odd and $a(n) = 2b(n)$, then n is a congruent number. If n is even and $a'(n) = 2b'(n)$, then n is a congruent number.

Example 2.12. (i) $a(1) = b(1) = 2, a(3) = b(3) = 4$ Hence, $a(1) \neq 2b(1), a(3) \neq 2b(3)$. Hence 1,3 are not congruent numbers.

(ii) $a'(2) = b'(2) = 2$. Hence 2 is not a congruent number.

Theorem 2.13. *If the weak Birch and Swinnerton-Dyer conjecture is true, then any positive integer* $n \equiv 5, 6, 7 \pmod 8$ *is a congruent number.*

Proof. Suppose $n \equiv 5, 6, 7 \pmod 8$ is a positive integer. Writing $n = a^2 b$ with b squarefree. Then a is odd, otherwise 4 would be a factor of n. Therefore, $n \equiv b \pmod 8$. Thus we may assume n is squarefree.

If $n \equiv 5, 7 \pmod 8$ is odd, since there is no integral solution to $2x^2+y^2 \equiv 5, 7 \pmod 8$, we have $a(n) = b(n) = 0$. Hence, $a(n) = 2b(n)$. If the weak BSD conjecture is true, then Tunnell's Theorem implies that n is a congruent number.

If $n \equiv 6 \pmod 8$ is even, then $2y^2 \equiv 6 \pmod 8$ has no integral solution, and so $a'(n) = b'(n) = 0$. Hence, $a'(n) = 2b'(n)$. If the weak BSD conjecture is true, then Tunnell's Theorem implies that n is a congruent number. □

References

[1] Keith Conrad. Lecture Note: *The Congruent Number Problem.*

[2] Leonard Eugene Dickson. *History of the Theory of Numbers*, Vol. 2 (1920), p. 462.

[3] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms* (GTM 97), Springer-Verlag (1984).

[4] Jerrold Bates Tunnell. *A classical diophantine problem and modular forms of weight 3/2.* Inventiones Mathematicae (1983) 72:323-334.