Congruent Numbers and Heegner Points

Shou-Wu Zhang

1. Problem

An anonymous Arab manuscript [1], written before 972, contains the following

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.*

Examples

1. 24 is a congruent:
$$5^2 + 24 = 7^2, \qquad 5^2 - 24 = 1^2.$$
So is 6:
$$\left(\frac{5}{2}\right)^2 + 6 = \left(\frac{7}{2}\right)^2, \qquad \left(\frac{5}{2}\right)^2 - 6 = \left(\frac{1}{2}\right)^2.$$
It is clear that it suffices to assume n has no square factors.
2. Leonard Pissano in 1220's was challenged by Emperor's scholars to show that 5,7 are congruent numbers:
$$5: \qquad \left(\frac{49}{12}\right)^2, \qquad \left(\frac{41}{12}\right)^2, \qquad \left(\frac{31}{12}\right)^2$$
$$7: \qquad \left(\frac{463}{120}\right)^2, \qquad \left(\frac{337}{120}\right)^2, \qquad \left(\frac{113}{120}\right)^2$$

Conjecture (Fibonacci). *1 is not a congruent number.*

It took 400 hundreds year until it was proved by Fermat using his method of *infinite descent*.

Triangular version

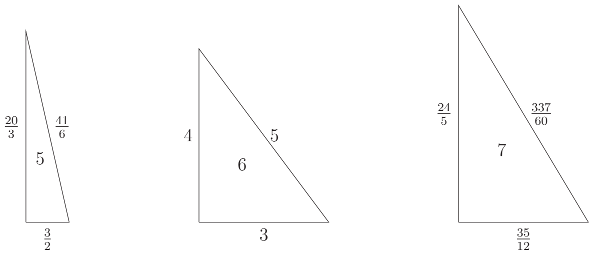
Congruent number problem (Triangular version). *Given a positive integer n, find a right angled triangle with rational sides and area n.*

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

The equivalence of the two forms is not difficult to prove: Suppose we are given an arithmetic progression $\alpha^2, \beta^2, \gamma^2$ with common difference n then we have the following right triangle with area n:
$$a = \gamma - \alpha, \qquad b = \gamma + \alpha, \qquad c = 2\beta.$$

Conversely given a right triangle $[a, b, c]$ with area n, then we have following progression with difference n:
$$\left(\frac{a-b}{2}\right)^2, \qquad \left(\frac{c}{2}\right)^2, \qquad \left(\frac{a+b}{2}\right)^2.$$

The following are right triangles respectively with areas 5, 6, 7:



2. 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, as the whole mystery of his method lay there. To quote Weil: "Fortunately, just for once he (Fermat) had found room for this mystery in the margin of the very last proposition of Diophantus".

Fermat's argument was based on the ancient Euclidean formula (300 BC): Given (a, b, c) positive integers, pairwise coprime, and $a^2 + b^2 = c^2$. Then there is a pair of coprime positive integers (p, q) with $p + q$ odd, such that
$$a = 2pq, \qquad b = p^2 - q^2, \qquad c = p^2 + q^2.$$

Thus we have a *Congruent number generating formula*:
$$n = pq(p+q)(p-q)/\square.$$

Here are some examples:

$$\begin{array}{lll} (p,q)=(2,1), & pq(p^2-q^2)=2\times 3, & n(2,1)=6; \\ (p,q)=(5,4), & pq(p^2-q^2)=5\cdot 4\cdot 9, & n(5,4)=5; \\ (p,q)=(16,9), & pq(p^2-q^2)=16\cdot 9\cdot 7, & n(16,9)=7. \end{array}$$

Theorem (Fermat). *1, 2, 3 are non-congruent.*

The following is the argument for 1 being a non-congruent number:

1. Suppose 1 is congruent. Then 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!

3. Conjectures

Following Goldfeld and BSD (Birch and Swinnerton-Dyer conjecture), we have the following conjecture concerning the distribution of congruent numbers:

Conjecture. *Let n be a square free positive integer.*

1. *If* $n \equiv 5,6,7 \mod 8$ *then n is congruent.*
2. *If* $n \equiv 1,2,3 \mod 8$ *then n has probability* 0 *to be congruent:*

$$\lim_{X\to\infty} \frac{\#\{n \le X : n = 1,2,3 \text{ mod } 8 \text{ and congruent}\}}{X} = 0.$$

Examples

1. Congruent numbers under 23:
$$n = pq(p+q)(p-q)/\square.$$
$$\begin{array}{ll} 14 \equiv 6 \mod 8 & (p,q) = (8,1); \\ 15 \equiv 7 \mod 8 & (p,q) = (4,1); \\ 21 \equiv 5 \mod 8 & (p,q) = (4,3); \\ 22 \equiv 6 \mod 8 & (p,q) = (50,49); \\ 13 \equiv 5 \mod 8 & (p,q) = (5^2\cdot 13, 6^2); \\ 23 \equiv 7 \mod 8 & (p,q) = (156^2, 133^2). \end{array}$$
2. Conjecturally, if $n \equiv 1,2,3$ mod 8 is congruent then *there are at least two very different ways* to construct triangles:
$$\begin{array}{lll} 34 \equiv 2 \mod 8, & (p,q) = (17,1), & (17,8); \\ 41 \equiv 1 \mod 8, & (p,q) = (25,16), & (41,9); \\ 219 \equiv 3 \mod 8, & (p,q) = (73,48), & (169,73). \end{array}$$

4. Theorems

The following are some results about the congruent and non-congruent numbers with specific prime factors.

Congruent primes

Theorem (Genocchi (1874), Razar (1974)). *A prime p (respectively 2p) is non-congruent if* $p \equiv 3 \mod 8$ *(respectively* $p \equiv 5 \mod 8$*).*

Theorem (Heegner (1952), Birch–Stephens (1975), Monsky (1990)). *A prime p (respectively 2p) is congruent if* $p \equiv 5,7 \mod 8$ *(respectively* $p \equiv 3 \mod 4$*).*

Zagier has computed a precise triangle with prime area 157:

$$157 = \tfrac{1}{2}ab, \qquad a^2 + b^2 = c^2.$$

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

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

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

Congruent numbers with many prime factors

Theorem (Feng 1996, Li–Tian 2000, Zhao 2001). *For any positive integer k, and any* $j \in \{1,2,3\}$*, there are infinitely many non-congruent numbers n with k odd primes factors, and congruent to j mod 8.*

Theorem (Gross 1985, Monsky 1990, Tian 2012). *For any positive integer k, and any* $j \in \{5,6,7\}$*, there are infinitely many congruent numbers n with k odd primes factors, and congruent to j mod 8.*

5. Elliptic Curves

Congruent number problem (Elliptic curve version). *For a positive integer n, find a rational point* (x,y) *with non-zero y on the elliptic curve:*

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

The equivalence with the triangle version is given by:

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

The rational points on an elliptic curve form a group. The understanding of this group structure is a major question in modern number theory and arithmetic algebraic geometry. The following was conjectured by Poincaré in 1901.

Theorem (Mordell 1922). *Let C be an elliptic curve over $\mathbb{Q}$. Then*

$$C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus C(\mathbb{Q})_{\text{tor}}$$

for some $r > 0$, where $C(\mathbb{Q})_{\text{tor}}$ is a finite group.

L-series

Let Δ denote the discriminant of C and set

$$N_p = \#\{\text{solutions of } y^2 \equiv x^3 + ax + b \bmod p\}.$$

$$a_p = p - N_p.$$

$$L(C, s) = \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Then $L(C, s)$ is absolutely convergent for $\Re(s) > 3/2$ (Hasse), and has holomorphic continuation to $\mathbb{C}$ (Wiles, *et al.*).

An $1,000,000 prize problem by Clay Math Institute:

Conjecture (Birch and Swinnerton-Dyer). *The Taylor expansion of $L(C, s)$ at $s = 1$ has the form*

$$L(C, s) = c(s-1)^r + \textit{higher order terms}$$

with $c \neq 0$ and $r = \operatorname{rank} C(\mathbb{Q})$. In particular $L(C, 1) = 0$ if and only if $C(\mathbb{Q})$ is infinite.

Application to congruent numbers

1. The L-series $L(E_n, s)$ has a functional equation $s \to 2 - s$ with sign
$$\epsilon(n) = \begin{cases} 1 & n \equiv 1, 2, 3 \mod 8 \\ -1 & n \equiv 5, 6, 7 \mod 8. \end{cases}$$
This gives a partition $\mathbb{N} = S \coprod T$ according to $\epsilon = \pm 1$.
2. Conjecturally, 100% of $n \in S$ are non-congruent numbers.
This maybe be checked by computing the *Selmer groups* which is a modern version of the Fermat's infinite descent, *the only tool available for non-congruent numbers.*
3. Conjecturally, 100% of $n \in T$ are congruent numbers with solutions given by *Heegner points, the only tool available for congruent numbers.*

Tian's theorem

Theorem (Ye Tian). *Let $m \equiv 5, 6, 7$ be a square free number and consider $E^{(m)} : my^2 = x^3 - x$. Then*

$$\operatorname{rank} E^{(m)}(\mathbb{Q}) = 1 = \operatorname{ord}_{s=1} L(E^{(m)}, s)$$

provided the following condition verified:

1. *the order part $n = p_0 p_1 \cdots p_k$ with $p_i \equiv 1 \mod 8$ for $i > 1$.*
2. *the class group $\mathcal{A}$ of $K = \mathbb{Q}(\sqrt{-2n})$ satisfies*
$$\dim_{\mathbb{F}_2} (\mathcal{A}[4]/\mathcal{A}[2]) = \begin{cases} 1, & p_0 \equiv \pm 1 \mod 8 \\ 0, & p_0 \equiv \pm 3 \mod 8 \end{cases}$$

6. Heegner Method

Both Monsky and Tian have proven their theorem based on the original method of Heegner. Heegner published his paper in 1952 as a 59 years old nonprofessional mathematician. In the same paper, Heegner solved Gauss' class number one problem whose correctness was accepted by the math community only in 1969, four years after Heegner died.

Modular parametrization

Heegner's main idea of constructing solutions to $E : y^2 = x^3 - x$ is by using modular functions (analogous to parametrizing the unit circle using *trigonometric functions* $(\cos 2\pi t, \sin 2\pi t)$):

$$f : \quad \mathcal{H} := \{z \in \mathbb{C}, \Im z > 0\} \longrightarrow E(\mathbb{C}).$$

The same idea can be used to answer the question:

Question. *Why is $e^{\pi\sqrt{163}}$ an almost an integer?*

$$\begin{aligned} e^{\pi\sqrt{163}} &= 262537412640768743.99999999999925\ldots \\ &= 640320^3 + 744 - 74 \times 10^{-14}\ldots \end{aligned}$$

The answer lies in the algebraicity of the special values of modular functions just like trigonometric functions which are transcendental but take algebraic values at rational multiples of π. Modular functions are transcendental, but take algebraic values at quadratic points. For example:

$$j(z) = e^{-2\pi iz} + 744 + 196884 e^{2\pi iz} + 21493760 e^{4\pi iz} + \cdots$$

$$j((1 + \sqrt{-163})/2) = -640320^3 = -262537412640768000$$

Heegner point

Here are the precise steps of construction of Heegener points in Tian's paper: Define $E^{(m)}$: $my^2 = x^2 - x$, $m^* := (-1)^{(n-1)/2}m$.

1. Take a standard parametrization f:

$$X_0(32) \to E^{(1)}.$$

2. Take a CM point in $X_0(32) = \Gamma_0(32)\backslash\mathcal{H}$ by

$$P = \begin{cases} [i\sqrt{2n}/8], & n \equiv 5 \mod 8, \\ [(i\sqrt{2n}+2)/8] & n \equiv 6, 7 \mod 8 \end{cases}$$

3. Take $\chi : \mathrm{Gal}(H(i)/K) \longrightarrow \mathrm{Gal}(\sqrt{m^*})/K \simeq \{\pm 1\}$,
4. Define $P_m = \sum_{\sigma\in\mathrm{Gal}(H(i)/K)} f(P)^\sigma \chi(\sigma)$.

Then $P_m \in E(\mathbb{Q}(\sqrt{m^*})^- \simeq E^{(m)}(\mathbb{Q})$.

What Tian proves is the following non-vanishing statement of Heegner points:

Theorem (Ye Tian). *Assume the following condition verified:*

1. *The order part $n = p_0 p_1 \cdots p_k$ with $p_i \equiv 1 \mod 8$ for $i > 1$.*
2. *The class group $\mathcal{A}$ of $K = \mathbb{Q}(\sqrt{-2n})$ satisfies*

$$\dim_{\mathbb{F}_2}(\mathcal{A}[4]/\mathcal{A}[2]) = \begin{cases} 1, & p_0 \equiv \pm 1 \mod 8 \\ 0, & p_0 \equiv \pm 3 \mod 8 \end{cases}$$

Then

$$P_m \in 2^k E^{(m)}(\mathbb{Q}), \qquad P_m \notin 2^{k+1} E^{(m)}(\mathbb{Q}).$$

References

[1] L. E. Dickson, *History of Theory of Numbers*, Vol. 2 (1920), p. 462.

[2] Y. Tian, Congruent numbers and Heegner points, preprint, arXiv:1210.8231.

Shou-Wu Zhang

Princeton University, USA
shouwu@math.princeton.edu

Professor Shou-Wu Zhang (Chinese: 张寿武) obtained his basic degree in mathematics and master degree respectively from Sun Yat-Sen University and Chinese Academy of Sciences in 1983 and 1986. In 1991 he received his PhD (Columbia University) under the guidance of Professor Lucien Szpiro and Professor Gerd Faltings.

He was Assistant Professor in Princeton University (1994–1996), and Associate Professor in Columbia University (1996–1998), Professor in Columbia University (1998–2013) and he has been tenured as Professor at Princeton University since 2011.

Zhang's main contributions to number theory and arithmetical algebraic geometry are his theory of positive line bundles in Arakelov theory which he used to prove (along with E Ullmo) the Bogomolov conjecture, and also his generalisation of the Gross-Zagier theorem from elliptic curves to abelian varieties of GL(2) type over totally real fields. In particular, the latter result led him to a proof of the rank one Birch-Swinnerton-Dyer conjecture for abelian varieties of GL(2) type over totally real fields. He has also developed the theory of arithmetic dynamics.

The honours received by Zhang include Sloan Foundation Research Fellowship (1997), Morningside Gold Medal of Mathematics (1998), Guggenheim Foundation Fellowship (2009), and Elected Fellow of the American Academy of Arts and Sciences (2011). He was also an invited speaker at the International Congress of Mathematicians in 1998.