Congruent number problem

—A thousand year old problem

Maosheng Xiong

Department of Mathematics,
Hong Kong University of Science and Technology

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 $\Longleftrightarrow n \cdot \square$ 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:

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

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.

Elliptic curves $E/\mathbb{Q}$

An elliptic curve $E/\mathbb{Q}$ is given by

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q},$$

where

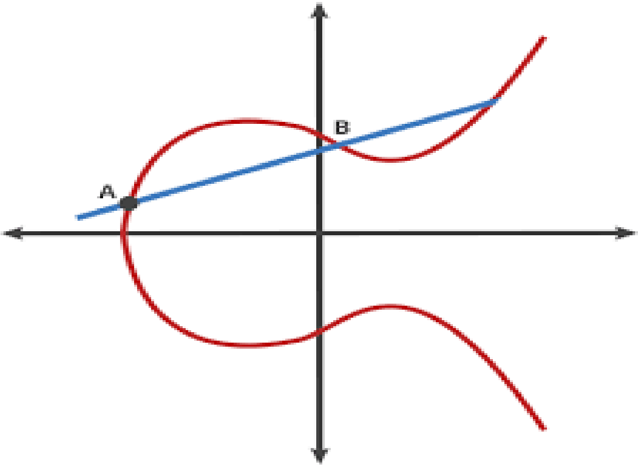
$$\triangle := -16(4a^3 + 27b^2) \neq 0.$$

Write

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \bigcup \{\infty\}.$$

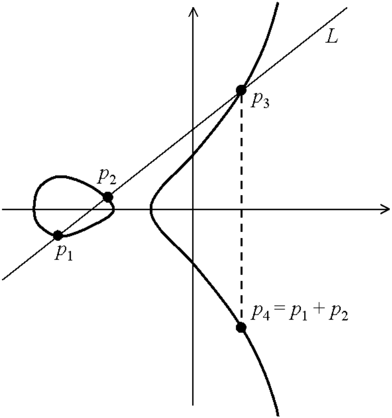
Basic Problem: Given an elliptic curve E, find all of its rational points $E(\mathbb{Q})$.

Elliptic curves $E/\mathbb{Q}$



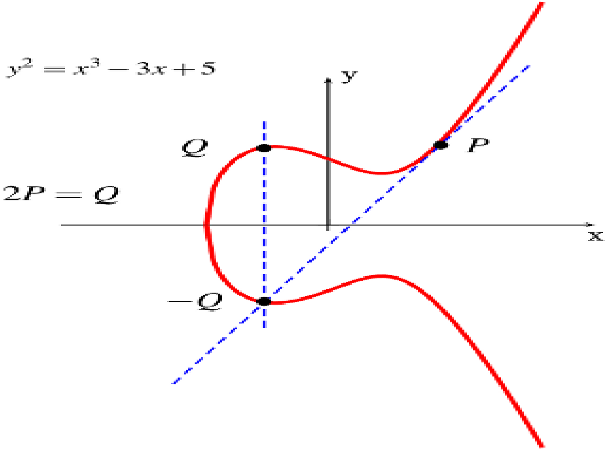
$$y^2 = x^3 - x + 1$$

Addition law



$$p_4 = p_1 + p_2, \quad p_3 = -p_4.$$

Addition law



$$Q = P + P = 2P.$$

Addition law on Elliptic curves $E/\mathbb{Q}$

Rule: $\mathcal{O} = \infty$ is the point "at infinity", which is on every vertical line.

Theorem (Poincare ($\approx$ 1900))

The addition law on $E(\mathbb{Q})$ has the following properties:

(a) $P + \mathcal{O} = \mathcal{O} + P = P$ *for all* $P \in E(\mathbb{Q})$.

(b) $P + (-P) = \mathcal{O}$ *for all* $P \in E(\mathbb{Q})$.

(c) $P + (Q + R) = (P + Q) + R$ *for all* $P, Q, R \in E(\mathbb{Q})$.

(d) $P + Q = Q + P$ *for all* $P, Q \in E(\mathbb{Q})$.

In other words, under the addition $E(\mathbb{Q})$ is an abelian group with identity $\mathcal{O}$.

A numerical example

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

The point $P = (1, 2)$ is on the curve $E(\mathbb{Q})$. Using the tangent line construction, we find that

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

Let $Q = \left(-\frac{7}{4}, -\frac{27}{8}\right)$. Using the secant line construction, we find that

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

Similarly,

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

Elliptic curves $E/\mathbb{Q}$

Theorem (Mordell (1922))

$E(\mathbb{Q})$ is a finitely generated abelian group, that is, there is a finite set of points $P_1, \dots, P_t \in E(\mathbb{Q})$ so that every point $P \in E(\mathbb{Q})$ can be written in the form

$$P = n_1 P_1 + n_2 P_2 + \cdots + n_t P_t$$

for some integers $n_1, n_2, \dots, n_t$.

A standard theorem about finitely generated abelian groups tells us that $E(\mathbb{Q})$ looks like

$$E(\mathbb{Q}) \cong (\text{Finite group}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}.$$

Structure of $E/\mathbb{Q}$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

- The finite group $E(\mathbb{Q})_{tors}$ is called the Torsion subgroup of $E(\mathbb{Q})$.
- The integer r is called the Rank of $E(\mathbb{Q})$.
- The description of all possible $E(\mathbb{Q})_{tors}$ is easy:

Theorem (Mazur (1977))

There are exactly 15 possible finite groups for $E(\mathbb{Q})_{\mathrm{tors}}$. In particular, $E(\mathbb{Q})_{\mathrm{tors}}$ has order at most 16.

Torsion points $E(\mathbb{Q})_{tors}$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

Theorem (Nagell-Lutz)

Let $E_{a,b}$ be an elliptic curve defined by

$$E_{a,b}: \quad y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ and $P := (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$ a nonzero torsion point of $E_{a,b}$. Then

(i) *$x, y \in \mathbb{Z}$ and*

(ii) *either $y = 0$, or else $y^2 | \triangle = 4a^3 + 27b^2$.*

Congruent number problem

Example:

- for the congruent number elliptic curve $E_n : ny^2 = x^3 - x$,

$$E_n(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

- Actually

$$E_n(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0), (\pm 1, 0)\}.$$

$$2(0,0) = 2(\pm 1, 0) = \mathcal{O},$$

$$(0,0) + (1,0) = (-1,0).$$

- However, determining the rank of $E_n(\mathbb{Q})$ is a very difficult question in the theory of elliptic curves in general.

Congruent number problem

Theorem

For a positive integer n, let E_n be the elliptic curve

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

Then n is a congruent number if and only if $r = \text{rank } E_n(\mathbb{Q}) > 0$, that is, there are infinitely many rational solutions (x, y) satisfying the equation of E_n.

Given an elliptic curve over $\mathbb{Q}$, determining the rank is one of the most important problems in the theory of elliptic curves.

Let $E : y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Q})$ be an elliptic curve with $\triangle = -16(4a^3 + 27b^2) \neq 0$. For any prime p, define

$$N_p = \# \text{ of solutions } (x, y) \text{ of } y^2 \equiv x^3 + ax + b \pmod{p},$$

$$a_p = p - N_p.$$

Theorem (Hasse (1922))

If $p \nmid \triangle$, then

$$|a_p| \leq 2\sqrt{p}.$$

Heuristic

Theorem (Hasse (1922))

If $p \nmid \triangle$, then

$$|a_p| \leq 2\sqrt{p}.$$

Heuristic argument:

- For each $x \pmod p$, there is a "50% chance" that the value of $f(x) = x^3 + ax + b$ is a square modulo p.
- If $f(x) = y^2$ is a square, then we (usually) get two points $(x, -y)$. Thus we might expect N_p is approximately

$$N_p \approx \frac{1}{2} \cdot 2 \cdot p = p.$$

Hence $|a_p| = |N_p - p|$ should be small compared with p.

L-series

- The L-series of E encodes all of the a_p values into a single function:

$$L(E, s) = \prod_{p \nmid 2\triangle} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

- The variable s is a complex variable $s \in \mathbb{C}$.
- $L(E, s)$ is absolutely convergent for $s \in \mathbb{C}$ when Re $(s) > \frac{3}{2}$, by Hasse's estimate $|a_p| \leq 2\sqrt{p}$.
- Wiles (with others) proved: $L(E, s)$ has holomorphic continuation to $\mathbb{C}$ (with a functional equation).

Behavior of L-series near $s = 1$

- A formal (completely unjustified) calculation yields

$$L(E,1) = \prod_p \left(1 - \frac{a_p}{p} + \frac{1}{p}\right)^{-1} = \prod_p \frac{p}{N_p}.$$

- This suggests that if N_p is large, then $L(E,1) = 0$.
- Birch and Swinnnerton-Dyer observed that if $E(\mathbb{Q})$ is infinite, then the reduction of the points in $E(\mathbb{Q})$ tend to make N_p larger than usual. So they conjectured

$$L(E,1) = 0 \quad \text{if and only if} \quad \#E(\mathbb{Q}) = \infty.$$

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

More generally, as the group $E(\mathbb{Q})$ gets "larger", the size of N_p seems to get larger too.

Conjecture (Birch and Swinnerton-Dyer)

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s).$$

That is, the Taylor expansion of $L(E,s)$ at $s=1$ has the form

$$L(E,s) = c(s-1)^r + \text{ higher order terms of } (s-1)$$

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

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

More generally, as the group $E(\mathbb{Q})$ gets "larger", the size of N_p seems to get larger too.

Conjecture (Birch and Swinnerton-Dyer)

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s).$$

That is, the Taylor expansion of $L(E,s)$ at $s=1$ has the form

$$L(E,s) = c(s-1)^r + \text{ higher order terms of } (s-1)$$

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

Theorem (Kolyvagin, Zagier+...)

The Birch and Swinnerton-Dyer conjecture is true if rank$(E(\mathbb{Q})) \leq 1$.

Tunnell's Theorem

Theorem (Tunnell 1983)

Let n be an odd squarefree positive integer. Consider the two conditions:

(A) *n is a congruent number;*

(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.*

Then

- *(A) implies (B).*
- *If the Birch and Swinnerton-Dyer conjecture is true, then (B) also implies (A).*

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

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

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

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

Application to congruent numbers

- If $n \equiv 5, 6, 7 \pmod 8$, the functional equation of the L-series implies that $L(E_n, 1) = -L(E_n, 1)$, hence $L(E_n, 1) = 0$.
- So conjecturally, 100% of $n \equiv 5, 6, 7 \pmod 8$ are *congruent numbers*.
- However to prove this requires finding infinitely many points on the elliptic curve.
- The points are given by Heegner points, the only tool available for congruent numbers.

Application to congruent numbers

- If $n \equiv 1, 2, 3 \pmod 8$, the functional equation of the L-series implies nothing: $L(E_n, 1) = L(E_n, 1)$.
- But conjecturally, "most likely" $L(E_n, 1) \neq 0$, hence 100% of $n \equiv 1, 2, 3 \pmod 8$ are *non-congruent numbers*.
- This may 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.

Conjectures

By the theory of elliptic curves, 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 $n \equiv 5, 6, 7 \pmod 8$ then n is congruent.*
2. *If $n \equiv 1, 2, 3 \pmod 8$ then n has probability 0 to be congruent:*

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

Examples

(Conjecture) If $n \equiv 5, 6, 7 \pmod 8$ then n is congruent.

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

- $14 \equiv 6 \pmod 8 \quad (p, q) = (8, 1);$
- $15 \equiv 7 \pmod 8 \quad (p, q) = (4, 1);$
- $21 \equiv 5 \pmod 8 \quad (p, q) = (4, 3);$
- $22 \equiv 6 \pmod 8 \quad (p, q) = (50, 49);$
- $13 \equiv 5 \pmod 8 \quad (p, q) = (5^2 \cdot 13, 6^2);$

Examples

Conjecturally, if $n \equiv 1, 2, 3 \pmod 8$ is congruent, then *there are at least two very different ways* to construct triangles:

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

- $34 \equiv 2 \pmod 8 \quad (p, q) = (17, 1), \quad (17, 8);$
- $41 \equiv 1 \pmod 8 \quad (p, q) = (25, 16), \quad (41, 9);$
- $219 \equiv 3 \pmod 8 \quad (p, q) = (73, 48), \quad (169, 73).$

Congruent primes

Theorem (Genocchi (1874), Razar (1974))

A prime p (respectively $2p$) is non-congruent if $p \equiv 3 \pmod 8$ (respectively $p \equiv 5 \pmod 8$).

Theorem (Heegner (1952), Birch-Stephens (1975), Monsky (1990))

A prime p (respectively $2p$) is congruent if $p \equiv 5, 7 \pmod 8$ (respectively $p \equiv 3 \pmod 4$).

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

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

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

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

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 prime factors, and congruent to $j \pmod 8$.

Theorem (Feng-X (2004))

Many new non-congruent numbers n...

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 prime factors, and congruent to $j \pmod 8$.

Selmer groups and Tate-Shafarevich groups

Let $\phi : E \to E'$ be an isogeny between two elliptic curves over $\mathbb{Q}$. Then Galois cohomology yields an exact sequence

$$0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[\phi] \longrightarrow 0$$

- $\#\left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right)$ is directly related with the rank of E over $\mathbb{Q}$.
- $Ш(E/\mathbb{Q})$ is very mysterious.
- $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ is a "local" object and can be computed in principle, is essentially Fermat's infinite descent.

2-descent and 2-Selmer groups

Let

$$\begin{array}{cccc} \phi: & E_n & \longrightarrow & E'_n : y^2 = x^3 + 4n^2 x \\ & (x, y) & \mapsto & \left(\frac{y^2}{x^2}, -\frac{y(n^2+x^2)}{x^2} \right) \end{array}$$

- ϕ is a 2-isogny as $\deg \phi = 2$.
- Let $\hat{\phi} : E'_n \to E_n$ be the dual isogeny of ϕ.
- Then ϕ and $\hat{\phi}$ induce two short exact sequences involving $\mathrm{Sel}^{(\phi)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi})}(E'_n/\mathbb{Q})$, which can be computed explicitly in principle.

2-descent and 2-Selmer groups

- Define

$$r(n) = \mathrm{rank}(E_n(\mathbb{Q})),$$

$$\#\mathrm{Sel}^{(\phi)}(E_n/\mathbb{Q}) = 2^{s(n,\phi)}, \quad \#\mathrm{Sel}^{(\hat{\phi})}(E_n'/\mathbb{Q}) = 2^{s(n,\hat{\phi})+2},$$

- The exact sequences imply that

$$r(n) \leq s(n,\phi) + s(n,\hat{\phi}).$$

- Consequence: if $s(n,\phi) = s(n,\hat{\phi}) = 0$, then $r(n) = 0$, i.e., n is a non-congruent number.
- This is the "2 descent" method.

2 descent and non-congruent numbers

Theorem (Non-congruent numbers)

(1) *(Genocchi 1855)*

$$\begin{array}{lll} n = p, & p \equiv 3 & \pmod 8; \\ n = pq, & p \equiv q \equiv 3 & \pmod 8; \\ n = 2p, & p \equiv 5 & \pmod 8; \\ n = 2pq, & p \equiv q \equiv 5 & \pmod 8; \end{array}$$

2 descent and non-congruent numbers

Theorem (Non-congruent numbers)

(2) *(Lagrange 1974)*

$$\begin{array}{llll} n = pq, & (p,q) \equiv (1,3) & (\mathrm{mod} 8), & (\frac{p}{q}) = -1; \\ n = 2pq, & (p,q) \equiv (1,5) & (\mathrm{mod} 8), & (\frac{p}{q}) = -1; \\ n = pqr, & (p,q,r) \equiv (1,1,3) & (\mathrm{mod} 8), & \textit{satisfying } (*); \\ n = 2pqr, & (p,q,r) \equiv (1,1,5) & (\mathrm{mod} 8), & \textit{satisfying } (*); \end{array}$$

Condition $(*)$: *n can be written as $n = p_1p_2p_3$ or $n = 2p_1p_2p_3$ such that*

$$\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$$

2 descent and non-congruent numbers

Theorem

(3) *(Serf 1989)*

$$\begin{array}{llll} n = pq, & (p,q) \equiv (5,7) & \pmod 8, & (\frac{p}{q}) = -1; \\ n = pqr, & (p,q,r) \equiv (1,3,3) & \pmod 8, & (\frac{p}{q}) = -(\frac{p}{r}); \\ n = pqr, & (p,q,r) \equiv (3,5,7) & \pmod 8, & (\frac{q}{r}) = -1; \\ n = 2pqr, & (p,q,r) \equiv (1,5,5) & \pmod 8, & (\frac{p}{q}) = -(\frac{p}{r}); \\ n = pqrs, & (p,q,r,s) \equiv (5,5,7,7) & \pmod 8, & \textit{and} \end{array}$$

$$1 = \left(\frac{p}{r}\right) = -\left(\frac{p}{s}\right) = -\left(\frac{q}{r}\right); \quad \textit{or}$$

$$1 = -\left(\frac{p}{r}\right) = \left(\frac{p}{s}\right) = -\left(\frac{q}{s}\right); \quad \textit{or}$$

$$1 = -\left(\frac{p}{r}\right) = -\left(\frac{p}{s}\right), \quad \left(\frac{q}{r}\right) = -\left(\frac{q}{s}\right).$$

2 descent and non-congruent numbers

Theorem

(4) (Feng 1996)
Suppose $n \equiv 3 \pmod 8$, n has one prime factor congruent to 3 modulo 8 and all others congruent to 1 modulo 8. If the graph $G(n)$ is an odd graph, then n is a non-congruent number.

All the above theorems were obtained by checking that those conditions imply that

$$\#\mathrm{Sel}^{(\phi)}(E_n/\mathbb{Q}) = 1, \quad \#\mathrm{Sel}^{(\hat{\phi})}(E'_n/\mathbb{Q}) = 4.$$

Hence the rank is zero, and n is non-congruent.

References

The talk is based on the papers (especially the first one)

1. Shou-Wu Zhang, *Congruent numbers and Heegner points*, Asia Pacific Mathematics Newsletter, vol. 3, no. 2, April 2013.
2. Ye Tian, *Congruent numbers with many prime factors*, PNAS, vol. 109, no. 52, December 2012.
3. John H. Coates, *Congruent numbers*, PNAS, vol. 109, no. 52, December 2012.