Congruent Number Problem

John H. Coates

Abstract

The following article reproduces the notes of a lecture I gave on October 5, 2002, in the Enrichment Programme for the Young Mathematics Talent of the Department of Mathematics and the Institute of Mathematical Sciences of the Chinese University of Hong Kong. I am very grateful to the anonymous students who wrote these very detailed notes of my lecture.

1 Congruent number problem

Today I want to explain to you the oldest unsolved major problem in mathematics (called the **congruent number problem**). It can be traced back at least to the 10-th century in Arab manuscripts (Al-Kazin) but it is possibly much older. It turns out to be a beautiful example of the modern theory of the **arithmetic of elliptic curves**, but it is more accurate to say that this theory grew out of the study of this problem.

In the 17-th century, **Fermat** gave a wonderful proof of the first special case of this problem. I want to explain his proof to you today. It also led Fermat to his so called **Last Theorem** (now solved by Andrew Wiles). But the original congruent number problem remains unsolved, despite the fact that conjecturally there is a very simple and beautiful answer to it.

Basic Facts about Numbers

All the basic facts about numbers which we shall need were certainly known to the Greek mathematicians (Euclid, Pythagoras, ...). We recall the set of **integers**:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}.$$

Definition 1 *If a and d are integers with $d \neq 0$, we say d **divides** a (or d is a **divisor of** a) if we have $a = da'$ for some integer a'.*

e.g. 3 divides 12: $12 = 3 \cdot 4$.

Notation. $d|a$ means d divides a. We also say $a = da'$ is a **factorization** of a.

The positive integers

$$2, 3, 5, 7, 11, 13, 17, 19, \cdots$$

stand out because they have no factorizations except the trivial ones.

Definition 2 *We say a positive integer p is a prime if its only divisors are $\pm 1, \pm p$.*

Theoretically, it is obvious that we can write any integer as a product of powers of primes.

Basic Problem. Find a "fast" way of factoring large integers.

e.g. an integer with 200 digits.

This problem has important applications to **cryptography**.

Fundamental Theorem of Arithmetic.

Each integer $n > 1$ can be written as a product of powers of primes

$$n = p_1^{a_1} \cdots p_r^{a_r} \quad (p_i \ distinct),$$

*and this decomposition is **unique** up to order.*

The uniqueness is not at all obvious; it depends on Euclid's algorithm.

Corollary 1 (Existence of greatest common divisor)
Let $a_1, \cdots, a_n$ be any finite set of positive integers. Then there exists a unique positive integer d satisfying:
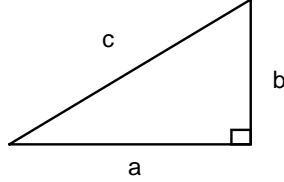
(i) $d|a_1, \cdots, d|a_n$;

(ii) *if e is any positive integer such that $e|a_1, \cdots, e|a_n$, then $e|d$.*

We call d the **greatest common divisor** of $a_1, \cdots, a_n$, and write

Notation. $d = (a_1, \cdots, a_n)$.

The oldest unsolved major problem in mathematics is concerned with **right-angled triangles** with sides a, b and c.


The basic result about these triangles is called Pythagoras' theorem, but it was certainly known in India before 800 B.C. (and so long before Pythagoras).

Pythagoras' Theorem.
$$a^2 + b^2 = c^2.$$

This theorem inexorably led to the introduction of **irrational numbers** once one accepts the idea that every **length** should be measured by a number e.g., a triangle with two perpendicular sides have length 1.
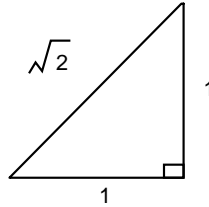

'$\sqrt{2}$' is the length of the hypothenuse of this triangle.

Definition 3 *We say a positive number α is rational if $\alpha = \frac{m}{n}$, where m and n are positive integers. We say α is irrational if α is not rational.*

Important Exercise. Use the fundamental theorem of arithmetic to prove that $\sqrt{2}$ is irrational.

Thus irrational numbers exist! It is the first step in creating larger systems of numbers in mathematics. Although it is not at all obvious, it turns out that π is irrational. But it is a much more "complicated" irrational number than $\sqrt{2}$. It is a transcendental number.

Notation: For simplicity, I am going to use the symbol Δ to denote the right-angled triangle with sides length a, b, c.
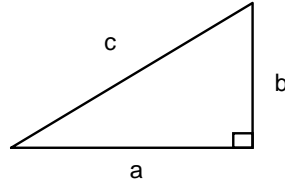
Usually, Δ will have at least one of its side lengths a, b, c irrational. But from long ago in the history of mankind it was noted that some triangles have all of a, b, c rational numbers. For example,
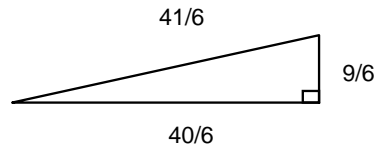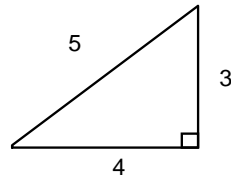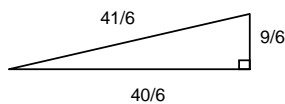

$$3^2 + 4^2 = 5^2,$$
$$\left(\frac{40}{6}\right)^2 + \left(\frac{9}{6}\right)^2 = \left(\frac{41}{6}\right)^2.$$

Definition 4 *We say Δ is rational if all three lengths a, b, c are rational.*
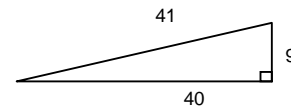
We also need an important subset of the rational triangles.

Definition 5 *We say Δ is primitive if all three of a, b, c are positive integers and $(a, b, c) = 1$.*

Exercise. Every rational Δ is similar to a unique primitive Δ. For example,

rational and similar to

Lemma 1 *Assume Δ is primitive, then precisely one of a and b is even.*

Proof. It all hinges on the fact that $a^2 + b^2 = c^2$.

(i) Assume $2|a$ and $2|b$, then $2|c$. But this contradicts our assumption that Δ is primitive.

(ii) Assume both a and b are odd, i.e., $a = 2a_1 + 1$, $b = 2b_1 + 1$. Then we get

$$a^2 + b^2 = 4k + 2, \quad \text{for some } k \in \mathbb{Z}.$$

Hence $2|c^2$ but 4 does not divide c^2. This contradicts the fundamental theorem. $\quad\square$

Proposition 1 *Assume Δ is **primitive**. Then there exist positive integers m, n with $(m, n) = 1$ such that*

$$a = n^2 - m^2, \ b = 2nm, \ c = n^2 + m^2,$$

or

$$a = 2nm, \ b = n^2 - m^2, \ c = n^2 + m^2.$$

Note. $(n^2 + m^2)^2 = (n^2 - m^2)^2 + (2nm)^2$.

Proof. Since Δ is primitive, say a is odd and b is even. Then c is odd and $(a, c) = 1$. Put

$$w_1 = \frac{1}{2}(c - a), \ w_2 = \frac{1}{2}(c + a).$$

Thus w_1 and w_2 are both positive integers. We will prove that w_1 and w_2 are relatively prime. Suppose $d|w_1$ and $d|w_2$. Then $d|w_1 + w_2$ and $d|w_2 - w_1$. But

$$w_1 + w_2 = c, \ w_2 - w_1 = a.$$

Hence $d = 1$ because $(a, c) = 1$. But we can rewrite $a^2 + b^2 = c^2$ as

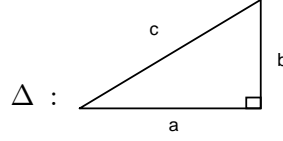$$(\frac{b}{2})^2 = w_1 w_2.$$

Hence w_1 and w_2 are relatively prime and their product is a square. Hence by the fundamental theorem each must be a square

$$w_1 = m^2, \ w_2 = n^2 \text{ and } (m, n) = 1.$$

This finishes the proof. $\quad\square$

Areas of Triangles. Our deep problem arises when we consider the **areas** of our right-angled triangles with sides length a, b and c, $a^2 + b^2 = c^2$. We all know that for

$$\text{Area}(\Delta) := \text{Area of } \Delta = \frac{1}{2}ab.$$

Now, suppose we fix a positive integer N. Clearly there exist always infinitely many Δ such that

$$\text{Area}(\Delta) = N$$

(just choose rational numbers a and b such that $ab = 2N$ and positive).

Key Question. Does there exist a **rational** Δ with $\text{Area}(\Delta) = N$?

Sometimes the answer is yes, e.g.

$N = 5$, right-angled Δ with sides: $\frac{9}{6}, \frac{40}{6}, \frac{41}{6}$; $\text{Area}(\Delta) = \frac{1}{2} \times \frac{40}{6} \times \frac{9}{6} = 5$.

$N = 6$, right-angled Δ with sides: $3, 4, 5$; $\text{Area}(\Delta) = \frac{1}{2} \times 3 \times 4 = 6$.

Definition 6 *We say N is* **congruent** *if there exists a* **rational** Δ *with Area$(\Delta) = N$.*

Note. This is a classical example of a **diophantine** problem. The problem has a trivial answer if we drop the hypothesis that Δ is rational.

Arab mathematicians (and possibly Indian mathematicians before them) made tables of integers which are congruent. They found

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47, \cdots$$

are all congruent.

Challenge. In each case you should try and find a rational Δ with

$$\text{Area}(\Delta) = N.$$

Remark 1 *If N is congruent and $N' = d^2 N$, where d is an integer, then N' is also congruent. So I have left out in the above list all integers which are of the form $d^2 N$, where N is already known to be congruent.*

Definition 7 *We say N is* **square free** *if $N = p_1 \cdots p_n$, where the p_i are distinct prime numbers.*

In looking, it suffices to consider only square free N.

Dilemna of the Ancients. Is 1 congruent ?

No one could find a rational Δ with $\mathrm{Area}(\Delta) = 1$. People began to try to prove that there was no such Δ, and many people falsely claimed a proof (e.g., Fibonacci).

Theorem 1 (Fermat) *1 is* **not** *a congruent number.*

Later in this talk, I want to tell you the marvellous proof found by Fermat. But first I want to discuss some related material.
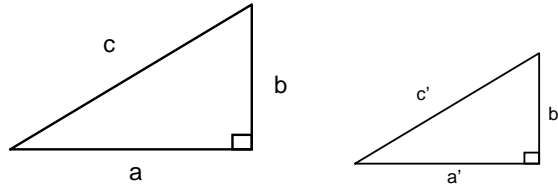
Corollary 2 *The equation $x^4 - y^4 = z^2$ has no solution in integers x, y, z with $xyz \neq 0$.*

Proof. (Assuming theorem) Suppose there is a solution in integers x, y, z with $xyz \neq 0$. Let
$$n = x^2, \; m = y^2.$$
Put $a = n^2 - m^2$, $b = 2nm$, $c = n^2 + m^2$ so that $a^2 + b^2 = c^2$ and the area of Δ with sides length a, b, c is

$$\mathrm{Area}(\Delta) = \frac{1}{2}ab = nm(n^2 - m^2) = x^2 y^2 z^2.$$

Take another Δ' with edges a', b', c' and parameter $\lambda = xyz$ (can assume x, y, z are all positive) so that
$$a' = \frac{a}{\lambda}, \; b' = \frac{b}{\lambda}, \; c' = \frac{c}{\lambda}$$
and $\mathrm{Area}(\Delta') = 1$, which shows that Δ' is rational and leads to a contradiction.
$\square$

In particular, the corollary shows that the equation

$$x^4 = y^4 + w^4$$

has no solution in integers x, y, w with $xyw \neq 0$. This is the only written evidence we have of what led Fermat to conjecture that, for any integer $n \geq 3$, the equation

$$x^n = y^n + z^n$$

has no solution in integers x, y, z with $xyz \neq 0$.

Returning to the problem of showing that integers N are not congruent, later mathematicians have used Fermat's ideas to find many others.

Non-Congruent square free N:

$$1, 2, 3, 10, 11, 17, 19, 26, 33, 35, 42, 43, \cdots .$$

Very extensive tables of both congruent and non-congruent numbers are known today, and are available on the web.

We can now state the two problems which remain unsolved !

Oldest Problem I. Prove that there is an algorithm (i.e. a procedure) for deciding in a finite number of steps whether a given positive integer N is congruent or not.

Oldest Problem II. Prove that every square free integer of the form

$$8n + 5 \ \ \text{or} \ \ 8n + 6 \ \ \text{or} \ \ 8n + 7 \quad (n = 0, 1, 2, \cdots)$$

is congruent.

These problems are one of the great challenges remaining in number theory, and probably in all of mathematics.
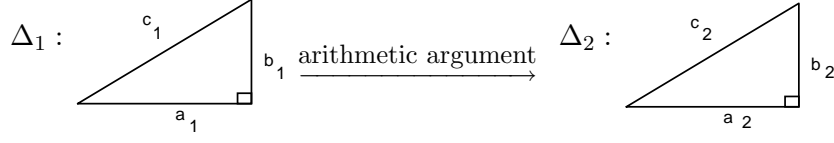
I hope to explain at the end of my lecture that *conjecturally* there is a very simple answer to both problems - if only we could prove it !

Proof of Fermat's Theorem.

Fermat's Theorem is equivalent to that there is no primitive triangle whose area is a square.

Remark 2 *When I say "square", I always mean the "square of an integer".*

Fermat introduced in the proof the fundamental idea of "infinite descent".

Key Step.

Δ_1 : [triangle with sides c_1, b_1, a_1] $\xrightarrow{\text{arithmetic argument}}$ Δ_2 : [triangle with sides c_2, b_2, a_2]

We always start with a *primitive* Δ_1 (with sides length a_1, b_1, c_1) whose area is a square and construct a new primitive Δ_2 (with sides length a_2, b_2, c_2) whose area is again a square and

Key Point: always $c_2 < c_1$. (In fact, we shall show that $c_2^4 < c_1$.)

Repeating the argument, we construct an infinite sequence of primitive Δ_i's whose area is always a square, and

$$c_1 > c_2 > c_3 > \cdots .$$

This gives a *contradiction* because one cannot have an infinite strictly decreasing sequence of positive integers.

Heart of the Argument. How do we construct Δ_2 from Δ_1 ?

Note. I will only speak about positive integers.

We know from our earlier lemma that there exist integers n_1, m_1 with $(n_1, m_1) = 1$ such that

$$a_1 = n_1^2 - m_1^2, \ b_1 = 2n_1m_1, \ c_1 = n_1^2 + m_1^2,$$

$$\text{Area}(\Delta_1) = n_1m_1(n_1 + m_1)(n_1 - m_1).$$

Claim. All four factors on the right are relatively prime in pairs.

Only have to worry about $n_1 + m_1$ and $n_1 - m_1$. If $d|(n_1 + m_1)$ and $d|(n_1 - m_1), d|2n_1$ and $d|2m_1$, which implies that $d = 1$ or 2. But $d = 2$ implies $2|a_1$ which is impossible since $2|b_1$ and so we would have $2|c_1$.

Key Conclusion. Since $\text{Area}(\Delta_1)$ is a square, we must have that each of the four factors

$$n_1, \ m_1, \ n_1 + m_1, \ n_1 - m_1$$

are squares (clear from unique factorization into primes). Hence there exist integers x, y, u, v such that

$$n_1 = x^2, \ m_1 = y^2, \ n_1 + m_1 = u^2, \ n_1 - m_1 = v^2.$$

Of course $(u, v) = 1$ and u, v are odd since $a_1 = u^2 v^2$ is odd. Also we have

$$u^2 = v^2 + 2y^2.$$

(Check: $(n_1 + m_1) = (n_1 - m_1) + 2m_1$.)

We can rewrite this last equation as

$$2y^2 = (u + v)(u - v). \tag{1}$$

Next Step. We carry out a second factorization with equation (1)

Claim. $(u - v, u + v) = 2$.

In fact, since u, v both odd, $2|u - v$ and $2|u + v$. If $d|u - v$ and $d|u + v$, we have $d|2u$ and $d|2v$, which leads $d|2$ since $(u, v) = 1$.

Hence unique factorization together with(1) that one of $u + v$ and $u - v$ must be of the form $2r^2$ and the other must be of the form $4s^2$, where r, s are integers. But we do not know which is of which form! But we still can say that
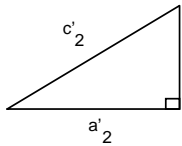
$$u = r^2 + 2s^2,$$
$$\pm v = r^2 - 2s^2,$$
$$y = 2rs.$$

But

$$x^2 = n_1 = \frac{1}{2}(u^2 + v^2) = r^4 + 4s^4.$$

(Check: $(r^2 + 2s^2)^2 + (r^2 - 2s^2)^2 = 2(r^4 + 4s^4)$.)

Now at last we can specify the triangle Δ_2:
First define

$$\Delta_2' : \qquad \text{right-angled}$$
$$(c_2')^2 = (a_2')^2 + (b_2')^2,$$

with

$$c_2' = x, \ a_2' = r^2, \ b_2' = 2s^2.$$

Key Observations.

(i) Area$(\Delta_2') = (rs)^2$ - a square !

(ii) $c_2' = x < c_1 = x^4 + y^4$ (in fact, $(c_2')^4 < c_1$).

If Δ_2' is not primitive, let $d = (a_2', b_2', c_2')$, we consider

$$
\Delta_2 : \qquad
\begin{array}{l}
a_2 = a_2'/d, \\
b_2 = b_2'/d, \\
c_2 = c_2'/d.
\end{array}
$$

Now Δ_2 is primitive and has all the desired properties ! We have proven Fermat's Theorem. $\square$

2   Birch-Swinnerton-Dyer conjecture

In the rest of today's lecture, I would like to talk about a deep conjecture related to the **Oldest Problem I** and **II** which we have mentioned before. The conjecture originated from B. Birch and H.P.F. Swinnerton -Dyer [1] in the 60's and was put in a simpler form by the work of J.B. Tunnell [3] in the 80's.

To begin with, let us consider the formal power series

$$\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_n T^n + \cdots$$

in T whose coefficients lie in $\mathbb{Z}$. We just add and multiply these formal power series as though they were polynomials in T with coefficients in $\mathbb{Z}$ (we are not concerned at all here with questions of convergence). For example, to multiply two such series

$$h(T) = \sum_{n=0}^{\infty} \alpha_n T^n, \quad k(T) = \sum_{n=0}^{\infty} \beta_n T^n$$

we simply pick any integer $r \geq 0$, and chop them off after the term in T^r, getting

$$h_r(T) = \sum_{n=0}^{r} \alpha_n T^n, \quad k_r(T) = \sum_{n=0}^{r} \beta_n T^n.$$

We then multiply the two polynomials $h_r(T), k_r(T)$. We see immediately the terms $T^0, T^1, \cdots, T^r$ in this product determine the terms of the same degree in $h(T)k(T)$. Moreover, it is clear that you can easily work out these terms by hand once you know the coefficients $\alpha_0, \cdots, \alpha_r$ and $\beta_0, \cdots, \beta_r$.

Now I also need to consider a formal infinite product as a power series in T with coefficients in $\mathbb{Z}$. For each integer $r \geq 1$, let us consider the polynomial in T with coefficients in $\mathbb{Z}$ defined by

$$g_r(T) = T \prod_{n=1}^{r} (1 - T^{8n})(1 - T^{16n})$$

Clearly,

$$g_{r+1}(T) - g_r(T) = g_r(T)((1 - T^{8(r+1)})(1 - T^{16(r+1)}) - 1)$$
$$= T^{8(r+1)+1} + \text{ terms of higher degree.}$$

In other words, $g_{r+1}(T)$ and $g_r(T)$ agree in all terms $T^0, \cdots, T^{8(r+1)}$. Thus it clearly makes sense to talk about $g(T) = \lim_{r \to \infty} g_r(T)$ as a well defined formal power series in T with coefficients in $\mathbb{Z}$. Informally, we can write

$$g(T) = T \prod_{n=1}^{\infty} (1 - T^{8n})(1 - T^{16n})$$

where the meaning of the infinite product is explained above. Let $j = 1$ or 2, and define the formal power series

$$\theta_j(T) = 1 + 2 \sum_{n=1}^{\infty} T^{2jn^2}.$$

We now consider the two products of formal power series

$$g(T)\theta_1(T) = \sum_{n=1}^{\infty} a(n)T^n,$$
$$g(T)\theta_2(T) = \sum_{n=1}^{\infty} b(n)T^n.$$

In other words, the integers $a(n)$ and $b(n)$ are defined to be coefficients when we take these products. It is clear that you can systematically work out the values of $a(n)$ and $b(n)$ for any given n by a simple finite calculation (in other words, there is a simple algorithm for finding them). Here is a sample of the values you will find.

a(1)=1	b(1)=1
a(3)=2	b(3)=0
a(5)=0	b(5)=2
a(7)=0	b(7)=0
a(11)=-2	b(11)=0
a(13)=0	b(13)=-2
a(15)=0	b(15)=0
a(17)=-4	b(17)=0
a(19)=-2	b(19)=0
a(21)=0	b(21)=-4
a(23)=0	b(23)=0

Table of values of $a(n)$ and $b(n)$ for n square free, $n \leq 23$.

As an exercise, I suggest you extend this table up to all square free $n < 100$.

I wonder if someone has noticed something miraculous in this table? In fact, for n square free and $n \leq 23$ it verifies the following:

Deep Conjecture. (Birch-Swinnerton-Dyer-Tunnell) *Let N be any odd square free positive integer. Then*

(i) *N is congruent if and only if $a(N) = 0$,*

(ii) *2N is congruent if and only if $b(N) = 0$.*

If the conjecture is true, it clearly answers our Problem I since I have already explained that there is a simple algorithm for calculating $a(N)$ and $b(N)$ in a finite number of steps. It can also easily be shown to answer Problem II. I leave this as an exercise for you.

Let me end by telling you what we know about this conjecture. In fact, the implication in one direction was proven long ago by Andrew Wiles and myself, see[2].

Theorem 2 (Coates-Wiles) *Let N be an odd square free positive integer. If $a(N) \neq 0$, then N is not congruent. If $b(N) \neq 0$, then 2N is not congruent.*

Our proof relies on ideas that have their origin in Fermat's proof. The great challenge to number theory is to prove the implication in the other direction !

I want to end with one other mysterious observation. If you compute $a(N)$ and $b(N)$, when N is odd and square free, and you find them to be non-zero you find the surprising fact that they are divisible only by small primes. In fact, if

you look at N square free with $N < 10^8$, the largest prime which occurs in an $a(N) \neq 0$ is the prime 349. In fact, there would be great theoretical interest in showing that there exist arbitrarily large primes dividing $a(N) \neq 0$, where N is square free, and similarly for $b(N)$. It is just possible that this could be done by ingenious elementary arguments. Let me leave this with you as a final unknown challenge!

References

[1]   Birch, B. and Swinnerton-Dyer, H., Notes on elliptic curves II,Jour urn. reine u. angewandte Math. 218 (1965),79–108.

[2]   Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39 (1977), no. 3, 223–251.

[3]   Tunnell, J. B., A classical Diophantine problem and modular forms of weight 3/2. Invent. Math. 72 (1983), no. 2, 323–334.

[4]   John Coates and S. T. Yau, Elliptic curves, modular forms & Fermat's last theorem. Proceedings of the Conference on Elliptic Curves and Modular Forms held at the Chinese University of Hong Kong, Hong Kong, December 18–21, 1993. Second edition. International Press, Cambridge, MA, 1997. iv+340 pp.MR1605709 (99d:11002).

Department of Pure Mathematics and Mathematical Statistics Cambridge University U.K.