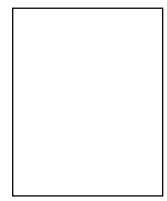
The Congruent Number Problem

V Chandrasekar

In Mathematics, especially number theory, one often comes across problems which arise naturally and are easy to pose, but whose solutions require very sophisticated methods. What is known as 'The Congruent Number Problem' is one such. Its statement is very simple and the problem dates back to antiquity, but it was only recently that a breakthrough was made, thanks to current developments in the Arithmetic of elliptic curves, an area of intense research in number theory.



V Chandrasekar was a research scholar in School of Mathematics, Tata Institute of Fundamental Research during 1974–85. He has taught mathematics for a considerable number of years at all levels. At present he is working for a computer firm.

Introduction

A positive integer n is called a **congruent number** if there exists a right angled triangle whose sides are rational numbers and whose area is the given number n.

If we represent the sides of such a triangle by X, Y, Z, with Z as the hypotenuse, then by our definition a positive integer n is a congruent number if and only if the two equations

$$X^2 + Y^2 = Z^2, \quad \frac{XY}{2} = n$$

have a solution with X, Y, Z all rational numbers.

Examples:

1. Consider the right angled triangle with sides $X = 3, Y = 4, Z = 5$. Its area n is $XY/2 = 6$, so 6 is a congruent number. Here we are lucky to find a suitable triangle for the number 6 whose sides are actually integers. It will be seen that this is in general an exceptional circumstance.

2. Consider the triangle with sides $3/2, 20/3, 41/6$. This

is a right angled triangle (!) and its area is 5. Therefore 5 is a congruent number.

Question. Does there exist a right angled triangle with integral sides and area equal to 5?

Question. Is 1 a congruent number? (There is a lot of history behind this which will be narrated below.)

One can generate congruent numbers at will by making use of the identity

$$(X^2 - Y^2)^2 + (2XY)^2 = (X^2 + Y^2)^2$$

which corresponds to the right angled triangle with sides $X^2 - Y^2, 2XY$ and hypotenuse $X^2 + Y^2$. We substitute our choice of integer values for X and Y and obtain the congruent number $n = XY(X^2 - Y^2)$. For example, $X = 3, Y = 2$ yields the triangle with sides 5, 12, 13 and area 30. So 30 is a congruent number. For more examples refer to *Box 1.*

Now any positive integer n can be written as $n = u^2v$, where v has no square factors (v is a 'squarefree integer'). It is clear that n is a congruent number if and only if v is so; for

Box 1. Generating Congruent Numbers

Here p, q are arbitrary positive integers of opposite parity (that is, $p+q$ is odd), the congruent number n is the square free part of $pq(p^2-q^2)$, and the sides of the triangle are proportional to $p^2 - q^2$, $2pq$, $p^2 + q^2$.

Serial Number	p	q	n	Sides of the Triangle
1	3	2	30	$5, 12, 13$
2	4	3	21	$7/2, 12, 25/2$
3	5	4	5	$3/2, 20/3, 41/6$
4	9	4	65	$65/6, 12, 97/6$
5	25	16	41	$40/3, 123/20, 881/6$

the right angled triangle for v can be obtained from the corresponding one for n, if it exists, by scaling down by a factor of u. (Remember that we allow the side lengths to take fractional values!) So when deciding whether n is congruent or not, we may assume that n is a squarefree integer. This will be done in what follows.

Now we are ready to formulate

The Congruent Number Problem. *Given a positive integer n, is there a simple criterion which enables us to decide whether or not n is congruent?*

A few remarks are in order. To start with, if we restrict the sides of the triangle to integer values only, the question can be settled, at least in theory, in a finite number of steps. To see why, recall the equations

$$X^2 + Y^2 = Z^2, \quad \frac{XY}{2} = n.$$

Since X and Y are now integers, X and Y both divide $2n$. So to see if a solution exists, we let X run through the set of divisors of $2n$, let $Y = 2n/X$ and check whether X^2+Y^2 is a square integer. Thus the problem can be settled in a routine manner. For example, we can easily verify that there is no integral solution for the case $n = 5$. (Note however that we do know that 5 is a congruent number.)

But once we allow the sides to have rational values, the problem acquires an entirely different status. There is no obvious starting point, unlike the case of integer solutions discussed above. One could endlessly churn out congruent numbers following the method in *Box 1* without being certain when a given number n (or $n \times m^2$, for some integer m) will appear on the list. Continuing in this way would exhaust one's computing resources, not to mention one's patience! Also, this procedure is of no avail if n is not a congruent number.

To appreciate this better, consider the following right angled triangle with area 101 which was found by Bastien in 1914. This triangle has sides

$$X = \frac{711024064578955010000}{118171431852779451900},$$

$$Y = \frac{396727280603349500 3922}{11817143185277945 1900}$$

and hypotenuse

$$Z = \frac{2 \times 2015242462949760001961}{11817143185277945 1900}.$$

This is known to be the smallest solution (in terms of the sizes of the numerator and denominator) corresponding to the congruent number 101! The serial number of this triangle in the list in *Box 1* would exceed 10^{20}!

The above considerations force us to look for a more indirect approach in our search for a criterion for characterizing congruent numbers.

Here we have yet another instance of a problem in number theory which is simple to state yet has hidden depths. There have been instances when the solutions of such problems have emerged only centuries after being posed. In such instances, a lot of deep and beautiful mathematics gets generated as a result. A striking example from recent times is the proof of Fermat's last theorem by Andrew Wiles in 1995, which uses a mind-boggling variety of techniques from several fields in current mathematical research.

We shall see how the Congruent number problem falls into this category by giving a brief account of its history and the concepts and techniques that were used in the solution of this problem which is deceptively so simple to state.

Brief History

The congruent number problem makes its earliest appearance in an Arab manuscript traced to the tenth century (c 972 AD). In his classic *History of the Theory of Numbers*, Vol 2 (Diophantine Analysis), Dickson quotes Woepeck's view that there is no indication that the Arabs knew Diophantus prior to the translation by Aboul Wafi (998 A.D), but they may well have come across the problem from the Hindus who were already acquainted with his work. The

Arabs figured out that the following numbers are congruent: 5, 6, 14, 15, 21, 30, 34, 65, 70, 110, 154, 190 and so on. In fact, their list contains ten congruent numbers greater than 100, for example, 10374.

The scene later shifts to Pisa, where Leonardo Pisano (better known as Fibonacci), by virtue of his position as a mathematical expert in his native city, is presented to the Emperor Frederic II. The king's scholars challenge him to find three rational numbers whose squares form an arithmetic progression with common difference 5. This is equivalent to finding integers X, Y, Z, T, with $T \neq 0$, such that $Y^2 - X^2 = Z^2 - Y^2 = 5T^2$, and this in turn reduces to finding a right triangle with rational sides

$$\frac{Z+X}{T}, \frac{Z-X}{T}, \frac{2Y}{T}$$

and area 5; in other words, to the question of whether 5 is a congruent number or not. Leonardo addressed the general problem in his memoir *Liber Quadratorum* (1225), which was lost to the world till it was found and published by Prince Boncompaign in the year 1856. In addition to showing that 5 and 7 are congruent numbers (the triangles have sides $3/2, 20/3, 41/6$ and $35/12, 24/5, 337/60$ respectively), he also states without proof that no congruent number can be a square, or equivalently that 1 is not a congruent number.

The proof of this statement had to wait for four centuries. Eventually it led to Fermat's discovery of his method of infinite descent, which was to have a profound effect on subsequent developments in arithmetic, or number theory as we now call it.

Fermat had been in correspondence with many of his contemporaries regarding the existence of a right angled triangle with rational sides and a square area. An explicit reference to the application of his technique to prove that this is impossible appears in his letter to Huygens in 1659, where he states: "*As ordinary methods, such as are found in the books, are inadequate to proving such difficult propositions, I discovered at last 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". To apply it to affirmative questions is much harder, so that, when I had to prove that "Every prime of the form $4n+1$ is a sum of two squares", I found myself in a sorry plight. But at last such questions proved amenable to my method." [We infer that technique of infinite descent had its first application in number theory to the problem of congruent numbers.] Continuing, Fermat gives a cryptic description of his method: "*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*".

Before reproducing Fermat's proof we prove the following

Proposition 1. *Let X, Y, Z be the sides of an integer-sided right angled triangle, with Z the hypotenuse, such that X, Y, Z have no common factors. Then there exist relatively prime integers p, q such that $p+q$ is odd, $\{X, Y\} = \{p^2 - q^2, 2pq\}$ and $Z = p^2 + q^2$.*

Proof. Clearly X and Y cannot be both even, as they have no common factors. Both cannot be odd, for in this case both X^2 and Y^2 would be 1 modulo 4, implying that $Z^2 \equiv 2 \pmod 4$; but this is absurd as no square is of the form $2 \pmod 4$. Thus one of them, say X, is odd and the other, Y, is even. It follows that Z is odd and that $Z+X, Z-X$ are both even. Therefore $(Z+X)/2$ and $(Z-X)/2$ are integers; indeed they are coprime, because X and Z are themselves coprime.

Since $Y^2 = Z^2 - X^2$, we obtain:

$$\left(\frac{Y}{2}\right)^2 = \frac{Z+X}{2} \cdot \frac{Z-X}{2}.$$

By the unique factorization property of the integers, each factor on the right side must be a square. Thus $(Z+X)/2 =$

p^2, $(Z-X)/2 = q^2$ with p and q coprime. Solving, we obtain

$$X = p^2 - q^2,\ Y = 2pq,\ Z = p^2 + q^2.$$

Since X is odd, $p+q$ is odd. ∎

Fermat's Legacy

We now reproduce Fermat's proof by the method of descent of the following

Theorem. *1 is not a congruent number.*

Proof. Suppose, on the contrary, that 1 is a congruent number; i.e. there exists a right angled triangle with integral sides whose area is a square integer. In view of Proposition 1, its sides must be of the form $2pq, p^2 - q^2, p^2 + q^2$ with $p > q > 0$, $p+q$ odd and $(p,q) = 1$.

Since the area $(= pq(p-q)(p+q))$ is a square integer and the numbers $p, q, p-q, p+q$ are mutually coprime, it follows that *each* of these numbers is a square integer. We write

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

Since u and v are odd and coprime, it follows that the gcd of $u+v$ and $u-v$ is 2. But now we have

$$2y^2 = 2q = u^2 - v^2 = (u+v)(u-v).$$

Arguing as in Proposition 1, we see that there exist integers r, s such that $(u+v, u-v) = (2r^2, 4s^2)$ or $(u+v, u-v) = (4r^2, 2s^2)$. The former case leads to $u = r^2+2s^2$, $v = r^2-2s^2$ and therefore to

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

Hence $r^2, 2s^2, x$ are the sides of a right angled triangle with area $(rs)^2$ and hypotenuse $x = \sqrt{p} < p^2+q^2$ (the hypotenuse of the triangle with which we started). The case $u+v = 4r^2$, $u-v = 2s^2$ is dealt with in similar fashion.

So, starting from a right angled triangle with integral sides whose area is a square integer, we have produced another

triangle of the same type with a smaller hypotenuse than the original triangle. Clearly this process can be repeated. But this gives rise to an infinite decreasing sequence of positive integers–a clear absurdity. (This is the central principle behind infinite descent.) We are thus led to a contradiction and we conclude that 1 is not a congruent number. ∎

The non-congruent nature of the number 1 is of special interest because it shows that there is no non-trivial solution to the equation $X^4 - Y^4 = Z^2$, which in turn implies Fermat's last theorem ('The equation $X^n + Y^n = Z^n$ has no non-trivial solutions in integers for $n > 2$') for the case $n = 4$!

In the following two propositions we prove the claims made above.

Proposition 2. *A number n is congruent if and only if there exists a rational number a such that $a^2 + n$ and $a^2 - n$ are both squares of rational numbers.*

Proof. Let n be a congruent number and let X, Y, Z be rational numbers satisfying

$$X^2 + Y^2 = Z^2, \quad \frac{XY}{2} = n.$$

Then $X^2 + Y^2 \pm 2XY = Z^2 \pm 4n$, so

$$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n.$$

So if we take $a = Z/2$, then a is rational and $a^2 + n$ and $a^2 - n$ are both squares of rational numbers.

For the converse, let a be a rational number such that $a^2 + n$ and $a^2 - n$ are squares of rational numbers. Let

$$X = \sqrt{a^2 + n} + \sqrt{a^2 - n}, \quad Y = \sqrt{a^2 + n} + \sqrt{a^2 - n},$$

and

$$Z = \sqrt{X^2 + Y^2} = \sqrt{4a^2} = 2a.$$

Then X, Y, Z are the sides of a right angled triangle with rational sides and area $XY/2 = ((a^2 + n) - (a^2 - n))/2 = n$. ∎

Proposition 3. *If there are non-zero integers X, Y, Z such that $X^4 - Y^4 = Z^2$, then 1 is a congruent number.*

Proof. Write the equation in the form

$$X^4 = Y^4 + Z^2.$$

Using Proposition 1, we deduce that there exist integers p, q such that $X^2 = p^2 + q^2$ and $Y = p^2 - q^2$. But this leads to

$$\frac{p^2}{q^2} + 1 = \left(\frac{X}{q}\right)^2, \quad \frac{p^2}{q^2} - 1 = \left(\frac{Y}{q}\right)^2.$$

So p^2/q^2 is a rational number such that p^2/q^2+1 and p^2/q^2-1 are squares of rational numbers. In other words 1 is a congruent number. ∎

Combining Propositions 2 and 3 with the fact that 1 is a non-congruent number, we deduce Fermat's last theorem for $n = 4$.

Before closing this section, it is fitting to quote Weil's lavish praise of Fermat and his justly-famous method: "*The true breakthrough came in 1922 with Mordell's celebrated paper; here, if Fermat's name does not occur, the use of the words "infinite descent" shows that Mordell was well aware of his indebtedness to his remote predecessor. Since then the theory of elliptic curves, and its generalizations to curves of higher genus and to abelian varieties, has been one of the main topics of modern number theory. Fermat's name, and his method of infinite descent, are indissolubly bound with it; they promise to remain so in the future*".

Congruent Numbers and Elliptic Curves

Congruent numbers continued to excite the curiosity of number theorists over the years. Their congruence properties have been investigated and tables of such numbers constructed. Some classes of numbers have also been identified as congruent numbers. To cite an example, a result due to Heegner and Birch shows that if n is a prime number of the form 5 (mod 8) or of the form 7 (mod 8) then n is a congruent number. (See *Box 2.*)

But what is ultimately sought is a simple and complete characterization of all congruent numbers; in other words, an algorithm which will quickly determine whether a given natural number n is congruent or not.

Box 2. Some Classes of Congruent Numbers

This box displays some results given in the paper by K Feng [5]. It characterises some classes of congruent and non-congruent numbers in terms of their divisibility properties.

To illustrate, Gross's result states that if an integer n is square free and has at most two prime factors of the form 5, 6 or 7 (mod 8), then n is a congruent number.

If p and q are odd primes, then the Legendre symbol (p/q) is 1 if p is a quadratic residue modulo q (that is, if the equation $x^2 \equiv p \pmod{q}$ has a solution), else -1.

In the following account, n is taken to be a square free integer. The symbol '**CN**' means 'congruent number', while '**Non-CN**' means 'non-congruent number'. p, q, r denote distinct primes and p_i refers to an arbitrary prime congruent to i mod 8.

For **CN**

- $n = 2p_3$ (Heegner 1952, Birch 1968).
- $n = p_5,\ p_7$ (Stevens 1975).
- $n = p^u q^v \equiv 5, 6, 7 \pmod{8},\ 0 \leq u, v \leq 1$ (B Gross 1985).
- $n = 2p_3p_5,\ 2p_5p_7$.
- $n = 2p_1p_7$ with $(p_1/p_7) = -1$ (Monsky 1990).
- $n = 2p_1p_3$ with $(p_1/p_3) = -1$.

For **Non-CN**

- $n = p_3, p_3q_3, 2p_5, 2p_5q_5$ (Genocchi 1855).
- $n = 2p$ with $p \equiv 9 \pmod{16}$ (Bastien 1913).
- $n = p_1p_3$, with $(p_1/p_3) = -1$ (Lagrange 1974).
- $n = 2p_1p_5$ with $(p_1/p_5) = -1$.
- $n = p_1p_3q_1$ with $(p_1/p_3) = (p_3/q_1) = -1$.

As it happened, the search for such an algorithm was made possible by relating the congruent number problem to the arithmetic of elliptic curves.

This connection is established as follows. From Proposition 2 we know that a number n is congruent means there exists a rational square, say u^2 such that u^2+n and u^2-n are both rational squares. This implies that u^4-n^2 is a rational square, say v^2; or equivalently that $u^6-n^2u^2=u^2v^2$. Setting $x=u^2$ and $y=uv$ we arrive at the equation $y^2=x^3-n^2x$. Thus if n is a congruent number, we obtain a rational point (x,y) on the curve represented by the equation $y^2=x^3-n^2x$.

Now the curves corresponding to the equation $y^2=x^3-n^2x$ are examples of what are known as elliptic curves. The arithmetic of these curves has been a central topic of research in Number Theory over the years. In view of the above connection, it was natural to expect that the results relating to elliptic curves would be able to settle the congruent number problem. This expectation was realized when J Tunnell succeeded in finding a simple algorithm for the problem. (See *Box 3* for a brief outline of the logical steps involved in Tunnell's method.)

Let the reader be reassured that to apply the algorithm one does not need to know anything about elliptic curves, modular forms, liftings or L-functions which are (to name a few) some of the concepts and techniques which lie at the basis of Tunnell's work!

In what follows, $\#S$ denotes the number of elements of a set S.

Tunnell's Theorem (1983). *Let n be a square free congruent number (that is, n is the area of a right angled triangle with rational sides). Define A_n, B_n, C_n, D_n as follows:*

$$\begin{aligned}
A_n &= \#\{(x,y,z)\in \mathbf{Z}^3 \mid n=2x^2+y^2+32z^2\},\\
B_n &= \#\{(x,y,z)\in \mathbf{Z}^3 \mid n=2x^2+y^2+8z^2\},\\
C_n &= \#\{(x,y,z)\in \mathbf{Z}^3 \mid n=8x^2+2y^2+64z^2\},\\
D_n &= \#\{(x,y,z)\in \mathbf{Z}^3 \mid n=8x^2+2y^2+16z^2\}.
\end{aligned}$$

Then:

(A) $A_n = B_n/2$ *if* n *is odd; and*
(B) $C_n = D_n/2$ *if* n *is even.*

If the Birch–Swinnerton Dyer conjecture is true, then, conversely, these equalities imply that n *is a congruent number.*

Box 3. Elliptic Curves and the Congruent Number Problem

For each natural number n, let E_n denote the elliptic curve represented by the equation $y^2 = x^3 - n^2x$. Then we have the following correspondence between the set of right angled triangles with rational sides and area n and the set of rational points on E_n. Let the sides be A, B, C where A, B, C are rational and $A < B < C$, and let (x, y) be a rational point on E_n such that: (a) x is the square of a rational number, (b) the denominator of x is even, (c) the numerator of x has no common factor with n. The correspondence is given as follows:

$$(x, \pm y) \longrightarrow \left(\sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n},\ 2\sqrt{x}\right),$$
$$(A, B, C) \longrightarrow \left(\frac{C^2}{4},\ \pm\frac{(B^2 - A^2)C}{8}\right).$$

It can be shown by means of the above bijection that a number n is congruent if and only if there exist infinitely many rational solutions (x, y) on the elliptic curve E_n.

To each elliptic curve E_n, there is associated an important number $L(E_n)$, which we shall not attempt to define. It is known (this is the Coates–Wiles Theorem) that if E_n has infinitely many rational solutions, then $L(E_n) = 0$. Combining this with the remark in the previous paragraph we deduce the following: *If* $L(E_n)$ *is not zero, then* n *is a non-congruent number.*

The converse statement, namely that $L(E_n) = 0$ implies the existence of infinitely many rational points on E_n (in other words, that $L(E_n) = 0$ implies that n is congruent) would follow from a famous conjecture due to Birch and Swinnerton–Dyer. (This conjecture has been made for all elliptic curves, not just for the E_n defined above.)

Now Tunnell's work can be summarized in one line; he has found an expression for $L(E_n)$ which is of the form

$$L(E_n) = \begin{cases} C \times (A_n - B_n/2), & \text{if } n \text{ is odd,} \\ C \times (C_n - D_n/2), & \text{if } n \text{ is even} \end{cases}.$$

Here C is a non-zero number, and A_n, B_n, C_n, D_n are the quantities defined in the statement of Tunnell's theorem.

The justification of Tunnell's algorithm follows from the above mentioned facts.

Observe that Tunnell's algorithm helps one to establish whether a given number n is non-congruent.

Examples:

1. Let $n = 1$; then $A_n = B_n = 2$, so equation (A) is not valid. We conclude that 1 is not a congruent number.
2. We show similarly that 2 and 3 are not congruent numbers.
3. Let n be square free, odd and congruent to 5 or 7 modulo 8. Since $2x^2 + y^2$ can never be congruent to 5 or 7 modulo 8, both cardinalities in (A) are 0 and hence the condition is satisfied. If the Birch–Swinnerton Dyer conjecture were true, we would be able to conclude that any such n is a congruent number. (There is supportive argument for this statement from the tables and the vanishing of the so called L-value of the corresponding elliptic curve.)

In particular, 157 would be a congruent number. This is in fact true. A proof of this fact is furnished by the right angled triangle whose sides x, y, z, displayed below, were computed by Don Zagier. Again, this is the smallest solution for the area 157! The sides are X, Y where

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

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

and the hypotenuse is Z where

$$Z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967165700164808 30}.$$

A natural question on the part of the reader would concern the appropriateness of the word 'congruent' in the definition of congruent number. As to that, one cannot do better than to quote Richard Guy: *"Congruent Numbers are perhaps confusingly named"*.

But, after all, what's there in a name?

Suggested Reading

[1] R K Guy. ***Unsolved Problems in Number Theory.*** Springer-Verlag, 1981.

[2] N Koblitz. ***Introduction to Elliptic Curves and Modular Forms.*** Springer-Verlag, 1984.

[3] J Tunnell. A Classical Diophantine Problem and Modular forms of weight 3/2. ***Inventiones Math.*** 72. 323–33, 1983.

[4] A Weil. ***Number Theory: An Approach Through History.*** Birkhäuser, 1984.

[5] K Feng. ***Non-congruent Numbers, Odd graphs and the B-S-D Conjecture. Acta Arithmetica***, LXXV 1, 1996.

Address for Correspondence
V Chandrasekar
C/o Mr Sripathy
Spic Mathematics Institute
92, East-Coast Chambers
T. Nagar
Chennai 600 017, India.