Classroom

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

A Walk Which Must be Irrational for the Same Reason That 1 is Not Congruent

B Sury
Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560 059 India.
Email: sury@isibang.ac.in

A natural number is said to be a congruent number if it is the area of a right-angled triangle with rational sides. In another direction, Fermat showed that the equations $X^4 + Y^4 = Z^4$ and $X^4 - Y^4 = Z^4$ do not have nontrivial solutions in integers. He did this through a method now known as the 'method of descent'. In fact, he discovered this while working on the problem to determine which numbers are congruent. It turns out that the non-solvability of the above equations in non-zero integers is equivalent to the fact that 1,2 are not congruent numbers. We discuss this connection first. Following this, we show that a certain type of walk through a unit square cannot cover a rational distance for the same reason that 1 is not a congruent number.

Keywords
Congruent number, Diophantine equation, method of descent.

1. Introduction

The subject of Diophantine equations is an area of mathematics where solutions to very similar-looking problems

can vary from the elementary to the deep. Problems are often easy to state, but it is usually far from clear whether a given one is trivial to solve or whether it must involve deep ideas. Fermat showed that the equations $X^4+Y^4 = Z^4$ and $X^4-Y^4 = Z^4$ do not have nontrivial solutions in integers. He did this through a method now known as the *method of descent*. In fact, he discovered this while working on a Diophantine problem called the congruent number which we discuss below. There are other situations where these equations arise naturally. One such problem is the following (see *Figure* 1).

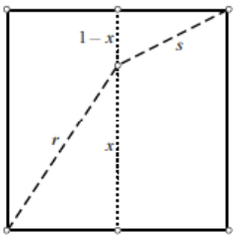

Figure 1.

Suppose we start walking from a corner of a unit square to reach the diagonally opposite corner. The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment until the middle line is reached and the other from that point to the opposite corner of the square. The question is whether we can follow such a path where both the segments we walked can be rational in lengths. This was asked (and answered!) by Roy Barbara [1]. We discuss this problem also.

2. The Congruent Number Problem

A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d; equivalently, if there exists an *arithmetic progression* of three terms which are all squares of rational numbers, the common difference being d, i.e., there exists a rational number x such that $x^2 - d$, $x^2 + d$ are squares of rational numbers.

Indeed, let $u \leq v < w$ be the sides of a right-angled

Fermat used the method of descent to show that the equations $X^4 + Y^4 = Z^4$ and $X^4 - Y^4 = Z^4$ do not have nontrivial solutions in integers. He discovered this while working on the congruent number problem.

The natural number *d* is congruent if and only if three squares of rational numbers are in an arithmetic progression of three terms with common difference *d*.

triangle with rational sides. Then $(v-u)^2/4$, $w^2/4$, $(u+v)^2/4$ form an arithmetic progression, so the choice $x = w/2$ fits.

Conversely, if $x^2 - d = y^2$, x^2, $x^2 + d = z^2$ are three rational squares in arithmetic progression, then $z - y$, $z + y$ are the legs of a right-angled triangle with rational legs, with area $(z^2 - y^2)/2 = d$ and rational hypotenuse $2x$ because $2(y^2 + z^2) = 4x^2$.

Examples

• 5, 6, 7 are congruent numbers. To see why, consider the following three right-angled triangles:

– with sides 3/2, 20/3, 41/6 with area 5;
– with sides 3, 4, 5 with area 6;
– with sides 35/12, 24/5, 337/60 with area 7.

• 1, 2, 3 are not congruent numbers.

The fact that 1, 2 are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4.

Indeed, if $a^2+b^2 = c^2$, $\frac{1}{2}ab = 1$ for some rational numbers a, b, c, then $x = c/2$, $y = |a^2-b^2|/4$ are rational numbers satisfying $y^2 = x^4 - 1$.

Similarly, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 2$ for rational numbers a, b, c, then $x = a/2$, $y = ac/4$ are rational numbers satisfying $y^2 = x^4 + 1$.

These equations reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat not to have nontrivial solutions, using the method of descent.

The unsolvability of $y^2 = x^4 \pm 1$ in rational numbers is exactly equivalent to showing 1, 2 are not congruent. In

fact $y^2 = x^4 - 1$ for rational x, y gives a right-angled triangle with sides y/x, $2x/y$, $(x^4+1)/xy$ and area 1.

Similarly, $y^2 = x^4 + 1$ for rational x, y gives a right-angled triangle with sides $2x$, $2/x$, $2y/x$ and area 2.

Remark

Here is an amusing way of using the above fact that 1 is not a congruent number to show that $\sqrt{2}$ is irrational!

Indeed, consider the right-angled triangle with legs $\sqrt{2}$, $\sqrt{2}$ and hypotenuse 2. If $\sqrt{2}$ were rational, this triangle would exhibit 1 as a congruent number!

Which numbers are congruent?

Though it is an ancient problem to determine which natural numbers are congruent, it was only in the late 20th century that substantial results were obtained and progress made which is likely to lead to its complete solution.

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$. Such equations define 'elliptic curves'. It turns out that:

> *d is a congruent number if, and only if, the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a rational solution with $y \neq 0$.*

In fact, $a^2 + b^2 = c^2$, $\frac{1}{2}ab = d$ implies that $bd/(c-a)$, $2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$.

Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y$, $2xd/y$, $(x^2 + d^2)/y$ and area d.

Though it is an ancient problem to determine which natural numbers are congruent, it is only in the late 20th century that substantial results were obtained and progress has been made which is likely to lead to its complete solution.

The natural number d is congruent if and only if the elliptic curve $y^2 = x^3 - d^2x$ has a rational point of infinite order.

In a nutshell, here is the reason we got this elliptic curve. The real solutions of the equation $a^2 + b^2 = c^2$ define a surface in 3-space and so do the real solutions of $\frac{1}{2}ab = d$. The intersection of these two surfaces is a curve whose equation in suitable coordinates is the above curve.

3. A Rational Walk Which is Impossible

Now, we discuss a problem which, on the face of it, is very different, but leads to the same impossibility problem as above. Recall the problem stated with reference to *Figure* 1.

Recall that the rule is to walk in a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment of length r until the middle line is reached and the other of length s from that point to the opposite corner. The question is whether we can follow such a path with both the distances r, s rational numbers. Suppose such a 'rational' path is possible. Let us call the vertical distance x on the middle line from the bottom to the point we reach on it. Of course, the rest of the vertical distance is $1 - x$. Now,

$$r^2 - \frac{1}{4} = x^2, \quad s^2 - \frac{1}{4} = (1-x)^2.$$

These give $2x = 1 + r^2 - s^2$, which is then rational. Then, writing $r = p/q$ and $s = u/v$, we have two equations

$$\frac{\sqrt{4p^2 - q^2}}{2q} = x, \quad \frac{\sqrt{4u^2 - v^2}}{2v} = 1 - x.$$

Therefore, since the above square-roots are rational, they must be integers and so, $q = 2Q$ (if q were odd, the number $4p^2 - q^2$ would be -1 modulo 4 which cannot be a square).

Thus,

$$x = \frac{\sqrt{p^2 - Q^2}}{2Q} = \frac{l}{2Q}$$

for some l with $(l, Q) = 1$.

Similarly, $v = 2V$ and

$$1 - x = \frac{\sqrt{u^2 - V^2}}{2V} = \frac{m}{2V}$$

with $(m, V) = 1$.

Thus,

$$1 = \frac{l}{2Q} + \frac{m}{2V}$$

which gives $2QV = lV + mQ$.

As $(l, Q) = 1 = (m, V)$, we get $Q|V$, $V|Q$; hence $Q = V$ as both are positive integers.

Hence, we have obtained $l^2 + Q^2 = p^2$, $m^2 + Q^2 = u^2$, $l + m = 2Q$ with $(l, Q) = 1 = (m, Q)$.

We show that this set of equations does not have any integral solutions. We could try to use a characterization of primitive Pythagorean triples and proceed but we take another approach. Now, the trivial identity $(l+m)^2 + (l-m)^2 = 2(l^2+m^2)$ gives, on multiplication by $(l + m)^2$:

$$(l + m)^4 + (l^2 - m^2)^2 = 2(l + m)^2(l^2 + m^2).$$

The reason to do this is that we have an expression in terms of p, u and Q as follows. Indeed, putting $l + m = 2Q$, $l^2 - m^2 = p^2 - u^2$ and $l^2 + m^2 = p^2 + u^2 - 2Q^2$, we have

$$16Q^4 + (p^2 - u^2)^2 = 8Q^2(p^2 + u^2 - 2Q^2).$$

It would be interesting to directly relate the above rational walk problem to the congruent number problem for 1 without going through Fermat's equation of degree four.

In other words,

$$4Q^4 - (p^2+u^2)Q^2 + \frac{(p^2-u^2)^2}{8} = 0.$$

This means that the discriminant $(p^2+u^2)^2 - 2(p^2-u^2)^2 = 6p^2u^2 - p^4 - u^4$ is a perfect square, say d^2. But then the general algebraic identity

$$(p^2+u^2)^4 - (6p^2u^2 - p^4 - u^4)^2 = (4pu(p^2-u^2))^2$$

tells us that $(p^2+u^2,\ d,\ 4pu(p^2-u^2))$ is an integer solution of the equation $X^4 - Y^4 = Z^2$. As we already saw, this equation has only the trivial solution in which $Y = 0$. Note that $d = (p^2+u^2)^2 - 2(p^2-u^2) \neq 0$ since $\sqrt{2}$ is irrational. Therefore, we have shown that a rational walk as above is impossible for the same reason that 1 is not a congruent number; viz., that the Fermat equation $X^4 - Y^4 = Z^2$ does not have integral solutions with $Y \neq 0$. It would be interesting to directly relate the above 'rational walk' problem to the congruent number problem for 1!

Suggested Reading

[1] **Roy Barbara, *The Mathematical Gazette*, Article 93.21, Vol.93, 2009.**

[2] **Keith Conrad, The congruent number problem, http://www.math.uconn.edu/~kconrad**

[3] **L E Dickson, *History of the Theory of Numbers*, Vol.II, Chelsea, New York, 1952.**

[4] **N Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd Ed., Springer-Verlag, New York, 1993.**

[5] **N M Stephens, Congruence properties of congruent numbers, *Bull. London Math. Soc.*, Vol.7, pp.182–184, 1975.**

[6] **J Tunnell, A Classical Diophantine Problem and Modular Forms of Weight 3/2, *Invent. Math.*, Vol.72, pp.323–334, 1983.**