Parabola Volume 28, Issue 1 (1992)

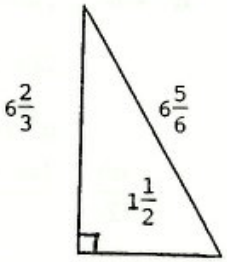
FROM PYTHAGORAS TO ELLIPTIC CURVES

Peter Brown*

There are few problems in 'elementary' mathematics which have not been solved. By 'elementary', I suppose I mean 'explainable to the person on the street'. Fermat's Last 'Theorem' is probably the best known of these, but there is another not so well known problem which dates back to the ancient Greeks and still has not been completely solved.

It is obvious that a right-angled triangle with sides 3, 4 and 5 has area 6. Now reverse the problem. Suppose I give you a positive integer, say 5, and ask you to construct a right triangle with **rational** sides whose area is 5. After some labour, you will find that a right triangle with sides $1\frac{1}{2}$, $6\frac{2}{3}$, $6\frac{5}{6}$ will do.

$$\left(1\tfrac{1}{2}\right)^2 + \left(6\tfrac{2}{3}\right)^2 = \left(6\tfrac{5}{6}\right)^2 \text{ and area } = \tfrac{1}{2} \times 1\tfrac{1}{2} \times 6\tfrac{2}{3} = 5.$$



Any positive integer N which is the area of a right triangle with rational sides is called a **congruent** number. Clearly 5 and 6 are congruent but it is shown by Fermat and Euler respectively that 1 and 4 are **not** congruent numbers. The big question, which the Greeks unsuccessfully tried to answer is: When is N congruent?

With the decline of learning in the West, much of the Greek mathematics passed to the Arabs, who reformulated the problem algebraically in the following way.

Can we find three rational squares in arithmetic progression with common difference N? For example, with $N = 6$, three such numbers are

$$\left(\frac{1}{2}\right)^2, \left(\frac{5}{2}\right)^2, \left(\frac{7}{2}\right)^2 \text{ since } \left(\frac{5}{2}\right)^2 - \left(\frac{1}{2}\right)^2 = \left(\frac{7}{2}\right)^2 - \left(\frac{5}{2}\right)^2 = 6.$$

To see the relationship between the two problems, suppose we have a right triangle with rational sides a, b, c and area $\dfrac{ab}{2} = N$, and consider the three rational squares

$$\left(\frac{b-a}{2}\right)^2, \left(\frac{c}{2}\right)^2, \left(\frac{a+b}{2}\right)^2.$$

*Peter is a pure mathematician at the University of New South Wales

Looking at the differences between successive terms,

$$\frac{c^2}{4} - \frac{(b-a)^2}{4} = \frac{c^2 - a^2 - b^2 + 2ab}{4} = \frac{ab}{2} = N$$

and $$\frac{(a+b)^2}{4} - \frac{c^2}{4} = \frac{ab}{2} = N,$$

so this sequence is an arithmetic progression with common difference N. Conversely if $x - N,\ x,\ x + N$ are three rational squares in arithmetic progression then we can write $x - N = u^2,\ x = v^2,\ x + N = w^2$ with u, v, w all rational.

Putting $$a = w - u,\ b = w + u,\ c = 2v$$

we have $$a^2 + b^2 = (w-u)^2 + (w+u)^2 = 2u^2 + 2w^2$$

$$= 2(x - N) + 2(x + N) = 4x = 4v^2 = c^2$$

$$\therefore a^2 + b^2 = c^2$$

and $$\frac{ab}{2} = \frac{(w-u)(w+u)}{2} = \frac{w^2 - u^2}{2} = \frac{(x+N) - (x-N)}{2} = N.$$

thus giving us the rational sides of a right triangle with area N.

For example: The Pythagorean triple $3, 4, 5$ leads to the arithmetic progression $\left(\frac{1}{2}\right)^2, \left(\frac{5}{2}\right)^2, \left(\frac{7}{2}\right)^2$ with $N = 6$ and $\left(\frac{7}{2}\right)^2, \left(\frac{13}{2}\right)^2, \left(\frac{17}{2}\right)^2$, with $N = 30$, gives the triad $(5, 12, 13)$.

The above calculations show that the Greek problem and the Arabic problem are equivalent, but unfortunately, this new problem was no easier to solve than the original one and the Arabs made little real progress on it.

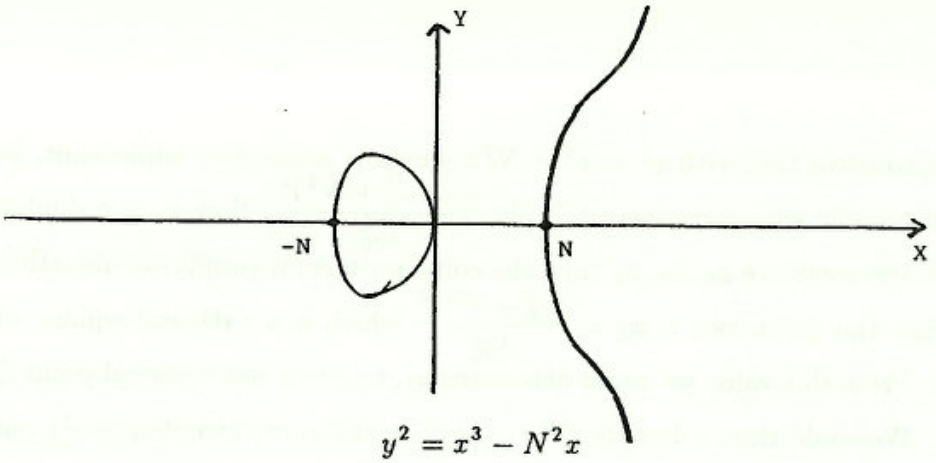
Elliptic Curves: Suppose we have our three rational squares in arithmetic progression with common difference N. We can write them as

$$x - N,\ x,\ x + N; \quad x \quad \text{a rational square.}$$

Now since these are squares, so is their product, call it y^2, so

$$y^2 = (x - N)x(x + N) = x^3 - N^2 x.$$

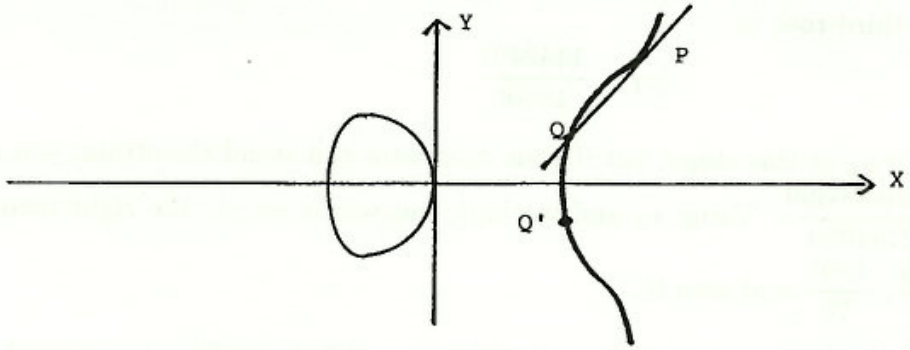
The curve given by $y^2 = x^3 - N^2 x$ is called an elliptic curve. (Don't confuse this with an ellipse!) It's graph is drawn below:



$y^2 = x^3 - N^2x$

This gives us another $1-1$ correspondence (well, almost!) between the sides of a rational right triangle of area N and points (with non-zero co-ordinates) **provided** the denominators of these co-ordinates are **even**; and the x-coordinate is a rational square. I will call these points **elliptic points**. If we can find elliptic points we can work backwards to get the triangle. For example the point $\left(\frac{25}{4}, \frac{35}{8}\right)$ lies on $y^2 = x^3 - 36x$, so this yields the arithmetic progression $\left(\frac{1}{2}\right)^2, \left(\frac{5}{2}\right)^2, \left(\frac{7}{2}\right)^2$, which in turns gets us back to our $3,4,5$ triangle.

The problem, however, of finding elliptic points seems worse than the original problem! It does, however, allow us to show that if there is one elliptic point (corresponding to one triangle), then there are infinitely many of them. To show this, we draw a tangent to the curve from $P(x_0, y_0)$ and see where it cuts the curve again at Q.



If you have studied implicit differentiation, you will be able to show that the slope of the tangent at (x_0, y_0) is $\frac{3x_0^2 - N^2}{2y_0}$, so the tangent has equation

$$y = y_0 + \left(\frac{3x_0^2 - N^2}{2y_0}\right)(x - x_0).$$

We now have to solve this with $y^2 = x^3 - N^2x$ which is somewhat unpleasant, but when we do, we get a cubic whose constant term is $\frac{-x_0^2(x_0^2+N^2)^2}{4y_0^2}$. Now x_0 is a double root of the cubic so if the roots are x_0, x_0, x_1 then the constant term is simply the negative of their product. Hence the third root is $x_1 = \frac{(x_0^2+N^2)^2}{4y_0^2}$ which is a **rational** square with even demoninator. From this value we could determine y_1, to give a new rational point $Q(x_1, y_1)$ on the curve. We could then calculate $Q'(x_1, -y_1)$ on the curve (see diagram!) and repeat the process as often as we like. (It is not obviously clear that we won't eventually get back to P at some stage, but in fact we never do). We see then, that if we can find one elliptic point, we can find infinitely many of them.

Example: The elliptic curve $y^2 = x^3 - 36x$ has elliptic point $P\left(\frac{25}{4}, \frac{35}{8}\right)$. (I got this from the 3,4,5 triangle).

Differentiating implicitly, $y' = \frac{3x^2-36}{2y} = \frac{1299}{140}$ at P. So the equation of the tangent at P is

$$y = \frac{35}{8} + \frac{1299}{140}\left(x - \frac{25}{4}\right)$$

or

$$y = \frac{1229}{140}x - \frac{6005}{112}.$$

Substitute into $y^2 = x^3 - 36x$, gives a cubic with constant term $-\left(\frac{6005}{112}\right)^2$. Now $\frac{25}{4}$ is a double root, so the third root is

$$x_1 = \frac{1442401}{19600}.$$

We don't really need y_1 at this stage, but if your calculator can stand the strain, you can show that $y_1 = \frac{1726556399}{2744000}$. Using x_1 and working backwards we get the right triangle with sides $\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}$ and area 6.

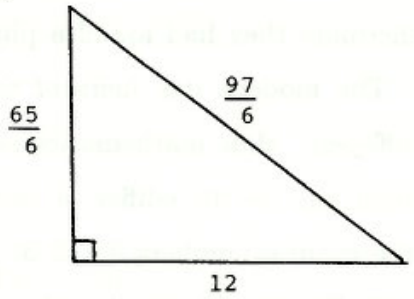
As you can see the arithmetic is fairly complicated, and I have still not answered the big question as to when N is congruent. The most recent result, that I am aware of, is due to J. Tunnell (1983) who made the following remarkable claim:
Consider the equation $2a^2 + b^2 + 8c^2 = N$, with a, b, c integers and N an **odd** positive integer.

If the number of non-negative **integer** solutions to this equation with c an odd number, equals the number of solutions with c even, then N is congruent.

Examples: If $N = 65$ $\quad 2a^2 + b^2 + 8c^2 = N$ has solutions

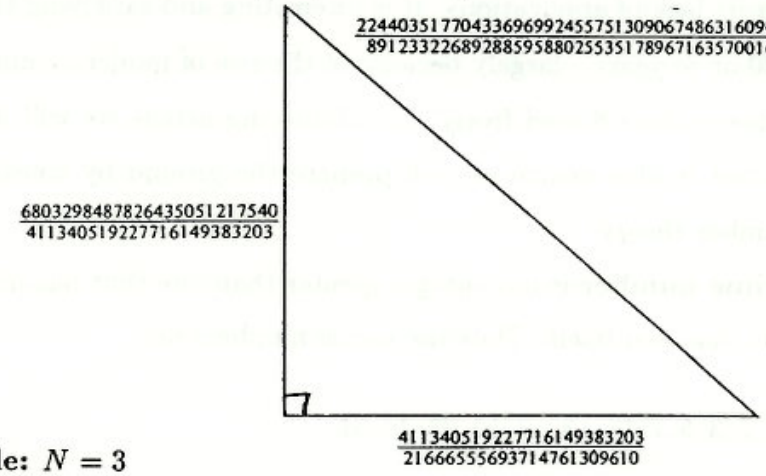
$$(a, b, c) = (4, 5, 1),\ (2, 7, 1),\ (4, 1, 2),\ (2, 5, 2)$$

so there are two solutions with c odd and two with c even and indeed 65 is congruent as the following triangle shows:



Area = 65

Example: If $N = 157$ $\quad 2a^2 + b^2 + 8c^2 = N$ has no integer solutions so the conditions are trivially satisfied, and again, N is congruent with 'simplest' triangle given below.



Example: $N = 3$

$2a^2 + b^2 + 8c^2 = N$ has solutions $(1, 1, 0)$ so 3 is **not** congruent.

No proof has yet been found for Tunnell's remarkable formula and so it remains a conjecture, and so the problem remains unsolved, although we have come a long way from the time of the ancient Greeks.